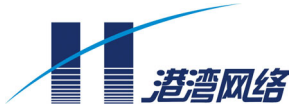
UniWorks DSL Center 用户手册

第一部分　　安装 UniWorks DSL Center 系统

第二部分　　配置 UniWorks DSL Center 系统



UniWorks DSL Center 用户手册

资料编号	P-1808****-20040520-100（手册编码尚未申请）
产品版本	V1.00
资料状态	发行

版权声明

© 港湾网络有限公司版权所有，并保留对本手册及本声明的最终解释权和修改权。

本手册的版权归港湾网络有限公司所有。未得到港湾网络有限公司的书面许可，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。

免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知。港湾网络有限公司在编写该手册的时候已尽最大努力保证其内容准确可靠，但港湾网络有限公司不对本手册中的遗漏、不准确或错误导致的损失和损害承担责任。

Users' Manual Copyright and Disclaimer

Copyright

© Copyright Harbour Networks Limited. All rights reserved.

The copyright of this document is owned by Harbour Networks Limited. Without the prior written permission obtained from Harbour Networks Limited, this document shall not be reproduced and excerpted in any form or by any means, stored in a retrieval system, modified, distributed and translated into other languages, applied for a commercial purpose in whole or in part.

Disclaimer

This document and the information contained herein is provided on an "AS IS" basis. Harbour Networks Limited may make improvement or changes in this document, at any time and without notice and as it sees fit. The information in this document was prepared by Harbour Networks Limited with reasonable care and is believed to be accurate. However, Harbour Networks Limited shall not assume responsibility for losses or damages resulting from any omissions, inaccuracies, or errors contained herein.

手册使用说明

读者对象

本手册的读者对象为安装和使用 UniWorks DSL Center 系统进行 DSLAM 设备集群管理的系统管理员。本手册需要读者熟悉以太网和组建局域网的概念和术语。

内容介绍

本手册详细介绍了 UniWorks DSL Center 系统的安装和使用方法，是 DSLAM 设备的系统管理员了解本系统并顺利完成系统安装与使用的指导文档。《UniWorks DSL Center 用户手册》共分为两个部分：

第一部分 安装 UniWorks DSL Center 系统

通过阅读本部分内容，用户将对本系统的用途、特点和版本信息等有一个全面的了解，并可进行本系统的正确安装。具体包括以下内容：

章序号	题目	内容描述
第1章	UniWorks DSL Center系统概述	简要讲述UniWorks DSL Center系统的功能、特点及版本说明。
第2章	系统构建	讲述UniWorks DSL Center系统的运行环境和安装、卸载方法。

第二部分 配置 UniWorks DSL Center 系统

通过阅读本部分内容，用户将了解使用本系统的相关知识，并可利用本系统完成若干 DSLAM 设备的集群管理。具体包括以下内容：

章序号	题目	内容描述
第3章	相关知识	讲述与使用本系统相关的网络基本知识及其它专业知识。
第4章	系统启动	介绍系统后台服务和管理服务器的组成、功能，以及如何启动它们，并进入管理系统。
第5章	设备管理	讲述设备管理的内容、相关技术原理和操作。
第6章	在线升级	讲述系统升级的方式及相关配置、操作。
第7章	事件管理	讲述事件管理的相关配置和操作。
第8章	安全管理	讲述安全管理的相关配置和操作。

第9章	业务配置向导	简要介绍如何通过业务配置向导完成系统的配置和管理。
附录A	系统管理和维护	讲述系统管理和维护时应注意的几个问题。
附录B	常见问题处理	讲述UniWorks DSL Center系统在使用中可能会遇到的问题及处理方法。

手册约定

手册中有关图标的约定如下：

图标	说明
 注意	这个图标表示提醒用户注意事项。
 提示	这个图标主要给出一些与正文相关的信息，同时给用户一些指引，协助用户更好的理解正文的内容。

获取技术支援

港湾网络有限公司建立了以总部技术支援中心、区域技术支援中心和本地技术支援中心为主体的完善的三级服务体系，并提供全天候 24 小时×365 天的电话热线服务。客户在产品使用及网络运行过程中遇到问题时请随时与港湾网络有限公司各地方的服务支持热线联系。请客户到www.harbournetworks.com获取各地服务支持热线电话。此外，客户还可通过港湾网络有限公司网站及时了解最新产品动态，以及下载需要的技术文档。

目录

第 1 章 UniWorks DSL Center 系统概述 1-1

1.1 简介 1-1

1.1.1 系统组成 1-1

1.1.2 系统特点 1-2

1.2 版本说明 1-3

第 2 章 系统构建 2-1

2.1 硬件环境 2-1

2.2 软件环境 2-1

2.3 UniWorks DSL Center 系统安装 2-2

2.3.1 Windows 版 2-2

2.3.2 与其它网管软件的配合安装 2-3

第 3 章 相关知识 3-1

3.1 概述 3-1

3.2 xDSL 和 DSLAM 简介 3-1

3.2.1 xDSL 3-1

3.2.2 DSLAM 3-2

3.2.3 IP DSLAM 3-3

3.3 网络基本知识 3-5

3.3.1 OSI（开放系统互联）参考模型 3-5

3.3.2 相关网络协议 3-6

3.3.3 网络硬件设备 3-10

3.4 操作系统 3-12

3.5 802.1x 协议 3-12

3.5.1 802.1x 体系结构 3-12

3.5.2 802.1x 认证机制 3-14

3.5.3 协议实现内容 3-16

3.5.4 与不支持 802.1x 的设备的兼容 3-19

3.6 RADIUS 协议 3-19

3.7 PPPoE 协议 3-20

第 4 章 系统启动 4-1

4.1 概述 4-1

4.2 启动后台服务 4-1
4.3 启动管理服务器前台 4-1
4.3.1 登录 4-2
4.3.2 前台主界面 4-2
第 5 章 设备管理 **5-1**
5.1 概述 5-1
5.2 设备信息管理 5-1
5.2.1 概述 5-1
5.2.2 发现或添加设备 5-1
5.3 图例 5-8
5.4 前进和后退 5-9
5.5 设备重新启动 5-9
5.6 保存设备 5-9
5.7 擦除设备 5-9
5.8 重启业务板 5-9
5.9 设备版本信息 5-10
5.10 板卡信息管理 5-10
5.11 CPU 利用率 5-10
5.12 Telnet 登录 5-11
5.13 端口管理 5-11
5.13.1 概述 5-11
5.13.2 选择端口 5-12
5.13.3 端口信息 5-14
5.13.4 认证管理 5-14
5.13.5 绑定管理 5-15
5.13.6 参数配置 5-20
5.13.7 模板配置 5-25
5.13.8 用户信息 5-30
5.14 VLAN 管理 5-32
5.14.1 概述 5-32
5.14.2 NormalVLAN 管理 5-33
5.14.3 SuperVLAN 管理 5-40
5.14.4 SubVLAN 管理 5-43
5.14.5 VID 使用模式 5-46

5.15 PPP 配置 5-47
5.15.1 概述 5-47
5.15.2 LCP 协商参数 5-48
5.15.3 NCP 协商参数 5-49
5.15.4 认证 5-50
5.15.5 其他配置 5-51
5.16 IP 地址获取方式 5-52
5.16.1 概述 5-52
5.16.2 IP 地址池 5-53
5.16.3 DHCP Client Proxy 5-55
5.17 802.1x 管理 5-57
5.17.1 概述 5-57
5.17.2 802.1x 管理 5-58
5.17.3 协议参数 5-59
5.17.4 重认证管理 5-59
5.17.5 异常下线检测 5-60
5.17.6 客户端软件升级 5-60
5.17.7 统计信息 5-60
5.18 RADIUS 管理 5-61
5.18.1 概述 5-61
5.18.2 基本配置 5-62
5.18.3 认证服务器 5-62
5.18.4 计费服务器 5-65
5.18.5 属性配置 5-65
5.18.6 CUT 配置 5-68
5.18.7 域管理 5-71
5.19 NAS 管理 5-73
5.19.1 概述 5-73
5.19.2 在线用户信息 5-74
5.20 静态路由 5-75
5.20.1 概述 5-75
5.20.2 创建 5-75
5.20.3 删除 5-76
5.20.4 刷新 5-76

5.21 访问控制 5-76
5.21.1 概述 5-76
5.21.2 设备访问控制配置 5-77
5.21.3 访问控制组管理 5-78
5.22 SYSLOG 配置 5-79
5.23 TRAP 配置 5-81
5.24 配置设备 PVC 服务 5-82
5.25 广播抑制 5-83
5.26 二层 PPPOE 配置 5-84
第 6 章 在线升级 6-1
6.1 概述 6-1
6.2 使用内置 FTP 服务器升级 6-1
6.3 指定 FTP 服务器 6-2
6.4 文件传输 6-2
6.4.1 参数设置 6-2
6.4.2 完成操作 6-3
第 7 章 事件管理 7-1
7.1 概述 7-1
7.2 文件菜单 7-2
7.3 查看菜单 7-2
7.4 工具菜单 7-3
7.4.1 搜索 7-3
7.4.2 服务器配置 7-4
7.4.3 SYSLOG 备份配置 7-5
7.4.4 SYSLOG 服务 7-5
7.4.5 TRAP 服务 7-5
第 8 章 安全管理 8-1
8.1 概述 8-1
8.2 用户组管理 8-1
8.2.1 增加用户组 8-2
8.2.2 删除用户组 8-2
8.2.3 配置用户组 8-2
8.3 用户管理 8-2
8.3.1 增加用户 8-3

8.3.2 删除用户 8-3
8.3.3 修改用户 8-3
8.4 SNMP 属性设置 8-4
8.4.1 默认配置 8-5
8.4.2 主机详细配置 8-5
8.5 保护设置 8-5
第 9 章 业务配置向导 9-1
9.1 概述 9-1
9.2 业务配置向导使用 9-1
9.2.1 启动业务配置向导 9-1
9.2.2 选择配置模式 9-1
9.2.3 二层透传配置 9-2
9.2.4 专线模式配置 9-3
9.2.5 认证方式配置 9-3
附录 A 系统管理和维护 A-1
附录 B 常见问题处理 B-1

第一部分

安装 UniWorks DSL Center 系统

1 UniWorks DSL Center 系统概述

1.1 简介

UniWorks DSL Center 系统是港湾网络有限公司推出的 DSLAM 设备管理软件产品，可以为港湾网络有限公司的 DSLAM 设备提供集群管理功能，大大减少用户的维护管理负担。同时针对目前市场应用需求，本产品还具有一定的业务管理能力，如批量放号、批量参数修改/配置等。

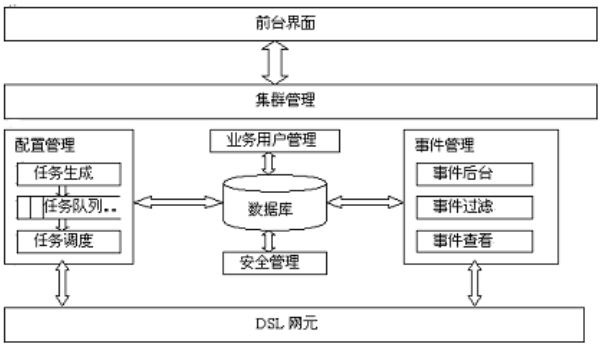
UniWorks DSL Center 系统采用异步、多任务的方式来支持批量操作，每个任务又可分成独立的子任务执行。

UniWorks DSL Center 系统支持网元级别的网管应用，管理工作界面采用左树右图（表）结构，简捷明了，便于用户进行系统的管理和配置。

1.1.1 系统组成

系统组成如下图所示：

图1-1 UniWorks DSL Center 系统组成



其中：

前台界面包括界面配置、功能管理和流程控制三部分：

- 界面配置模块提供一个 XML 文件，该文件定义了界面的菜单栏、工具栏、菜单项、菜单子项的属性以及各自的响应命令；
- 功能管理模块也提供了一个 XML 文件，定义了当前系统中支持的所有功能，每个功能对应文件中的两个字段：命令名和功能实现类；
- 流程控制模块响应用户的鼠标点击操作，把提取的命令名传递到功能管理模块中。

集群管理主要是集群的创建、配置（修改集群包含的设备）和删除，它只是针对“集群”，而不是集群的具体功能，它是在各个具体功能之上的一个概念。

业务用户管理包括业务用户开通/关闭、业务用户属性修改、业务用户查找等。在业务用户开通的管理中，可以提供界面用户进行端口上下行速率、端口认证方式等的配置。

配置管理主要包括各个功能项的配置，包括 802.1x、RADIUS、PPP 配置、IP 获取方式、广播抑制等，把用户的每一个集群配置都当成一项任务由任务后台来统一调度，并行下发到各个 DSL 网元设备执行，同时将结果返回前台界面。

事件管理包括日志和告警管理，事件的接收由事件后台统一负责，把接收到的事件存放到数据库中，用户可以根据各种查询条件查看事件。

安全管理是通过 UniWorks DSL Center 系统提供的用户管理创建用户组和用户，从而可以分别为每个用户组或用户指定不同的管理权限。安全管理同时也提供了设置设备访问团体的功能，只有本地设置的读写团体和设备上配置的读写团体一致时才能正确访问设备。同时只有 admin 用户组的用户才有权限登录安全管理，修改其他用户权限。

数据库主要是存放各种永久性数据，包括用户信息、事件数据等。

1.1.2 系统特点

UniWorks DSL Center 系统具有如下特点：

- UniWorks DSL Center 系统基于 JAVA 技术构建，支持跨操作系统平台的应用，可运行在 Microsoft Windows2000/XP、HP-UX、Solaris 等多种操作系统中；充分考虑了业务及功能拓展性，保护用户投资；

- 对每一个功能都提供了批量处理能力，减少用户配置管理负担；
- 对端口和 VLAN 等功能提供了集中管理功能，只要在一个界面上就可完成对设备的配置；
- 指定网段内的 DSLAM 设备发现功能，轻松拖拽就可加到集群中；
- 一体化的事件管理功能，用户可方便地在日志和告警之间进行切换，同时提供多种事件查询方式；
- 批量完成对设备系统文件、配置文件的升级和备份设备数据，节约用户时间。

1.2 版本说明

UniWorks DSL Center 系统的 V1.00 版支持多操作系统平台的应用，可运行在 Microsoft Windows2000/XP、HP-UX、Solaris 等多种操作系统，为 DSLAM 设备提供集群管理服务。

提示

本手册主要介绍 UniWorks DSL Center 系统 V1.00 的 Windows 版。

UniWorks DSL Center 系统的 V1.00 版本支持的设备种类包括：

- 港湾网络有限公司的 Hammer10000 IP DSLAM 接入交换机（以下简称 Hammer10000）。

提示

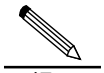
有关 Hammer10000 的说明及使用文档请参见 Hammer10000 的随机资料。

数据保存的基本方式包括：

- 数据库 MySql：用于用户信息及事件数据等的存储
- 提供 Windows 系统下的 TXT 及 Excel 文件格式的数据导入与导出

兼容性方面：

- UniWorks DSL Center 系统可以和港湾网络有限公司的网元管理软件 HammerViewV1.40 以及网络管理软件 EasyTouch 安装在同一台机器上。


提示

UniWorks DSL Center 系统与 HammerViewV1.40、EasyTouch 同机安装的相关说明请参见 2.3 节 “UniWorks DSL Center 系统安装”的相关内容。

2 系统构建

2.1 硬件环境

UniWorks DSL Center 系统安装在 PC 服务器上，其硬件配置要求如下：

- CPU 频率不小于 1.5GHz
- 硬盘容量不小于 40G 字节
- 内存不小于 512M 字节
- 具有网络连接设备

建议配置：

- HP PC Server ML-350 XEON 2.4G
- 40G SCSIHD
- 1024M 内存
- 100/1000M 以太网卡

2.2 软件环境

系统的软件环境主要包括：

- 操作系统：Windows 2000 Server / Professional（Service Pack 4）、Windows XP、HP-UX、Solaris 等
- 数据库：MySql

本手册有关界面及操作的讲解全部基于 Windows2000 Professional 操作系统。

2.3 UniWorks DSL Center系统安装

2.3.1 Windows版

1. 安装准备

请在安装 UniWorks DSL Center 系统之前，先确认计算机中安装的操作系统为 Windows 2000/XP 系列。如果不是，请先安装相应的操作系统之后再安装 UniWorks DSL Center 系统。

2. 进行安装

1） 用鼠标左键双击执行 setup.exe 安装文件，进入 UniWorks DSL Center 系统安装界面，提示用户将要安装 UniWorks DSL Center 系统；

2） 点击“Next”按钮，出现“许可证协议”窗口。用户必须认真阅读《港湾网络有限公司 UniWorks DSL Center 软件产品最终用户使用许可协议》内容。用户确认同意协议内容后，请点击“Yes”按钮，进行下一步安装，弹出“选择目的地位置”对话框；点击“No”按钮则退出安装；

3） 在“选择目的地位置”对话框中，用户可通过“浏览”按钮选择系统安装路径，请确定所选路径下具有足够的磁盘空间。系统默认安装路径为“C:\Program Files\HarbourNetworks\harbourNMS”；

注意

如果网管机上已经安装了港湾网络有限公司的其他网管软件，如 HammerView 和 EasyTouch，则在安装时不会出现安装路径选择框，直接和原有网管软件安装在同一个路径下。

4） 安装路径选好后，点击“下一步”按钮开始安装 UniWorks DSL Center 系统，用户可以看到系统安装进度条，此步骤需要几分钟的时间（具体时间因 PC 服务器的硬件配置及软件系统的不同而略有差异）；

5） 系统安装完成后，弹出“完成安装”对话框，提示用户是否立即重启计算机。用户可选择稍后重启计算机。此时用户点击“完成”按钮结束 UniWorks DSL Center 系统的安装。

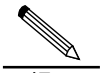
3. 安装检验

安装完成后，重新启动计算机，则可在 Windows 的‘开始’ －>‘程序’ 中看到 UniWorks DSL Center 系统程序组，包括：

- DSL Center
- Uninstall DslCenter

在‘我的电脑’ －>‘控制面板’ －>‘管理工具’ －>‘服务’中会看到：

- EasyTouch Event Service
- MySql



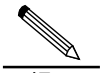
卸载说明：

1、用户可通过选择 Windows 的‘开始’－>‘程序’－>‘DslCenter’－> ‘Uninstall DslCenter’ ，或者通过双击执行相应的 setup.exe 安装文件－>进入 UniWorks DSL Center 卸载程序界面，按提示卸载 UniWorks DSL Center 系统。

2、卸载完成后，在原安装目录里系统还保留着一个目录：db，它存放着原先系统中的一些数据，如果不想保留这些数据，请手工删除这个目录。

2.3.2 与其它网管软件的配合安装

UniWorks DSL Center 系统可以和港湾网络有限公司的网元管理软件 HammerViewV1.40 以及网络管理软件 EasyTouch 安装在同一台机器上。在和 HammerView 同机安装时，请先安装 HammerView，然后再安装 UniWorks DSL Center 系统，否则可能会收不到 Trap 和日志。同样如果和 EasyTouch 共同安装在一台机器上时，也请先安装 EasyTouch，再安装 UniWorks DSL Center 系统。



建议 UniWorks DSL Center 系统不要与 HammerView 和 EasyTouch 安装在同一台机器上。

第二部分

配置 UniWorks DSL Center 系统

3 相关知识

3.1 概述

本章对 xDSL 技术、DSLAM 设备的用途和组网结构、IP DSLAM 提供的功能、网络基本知识及相关协议等进行了简要介绍。了解和掌握这些知识，将有助于您成功地使用 UniWorks DSL Center 系统。

3.2 xDSL和DSLAM简介

3.2.1 xDSL

随着国际互连网的快速发展，电子商务、电子政务等的应用，Internet 快速、高效、方便的特点已被人们所认识，网络已逐步成为人们工作、学习和生活必不可少的一部分。人们对通信的需求也从传统的电话、传真、音频、Modem 拨号上网等窄带业务逐渐向高速的 Internet 接入、可视电话、视频点播（VOD）等宽带业务领域延伸。 光纤到户（FTTH，Fiber-To-The-Home）虽然可以极大地提高整个网络性能，但其成本高，一时很难普及。如果能够把双绞铜线电话网包括进宽带接入网中，在普通电话线上实现电影、交互式电视、高密度图片的传输等多媒体业务，显然是一种节约成本、提高性能的想法，而且还可以充分利用电话网覆盖面广、现有敷设距离长等特点，实现大范围的应用推广。xDSL 技术就是在此背景下应运而生的。

xDSL 是 DSL(Digital Subscriber Line)的统称，意即数字用户线路，是以铜电话线为传输介质的点对点传输技术。包括：HDSL、SDSL、VDSL、ADSL 和 RADSL 等。其中 HDSL（High-bit-rate DSL，高比特率 DSL）、SDSL（Single-line DSL，HDSL 的单线版本）支持对称传输模式，主要应用于小型办公机构和家庭办公(SOHO)等从事电子商务和向局域网(LAN) 传送信息的环境，为这些用户的网络服务器提供上行和下行完全相同的传输带宽。VDSL（Very High Data Rate DSL，甚高速数字用户线）、ADSL（Asymmetric DSL，非对称 DSL）和 RADSL（Rate Adaptive DSL，速率自适应 DSL）支持非对称传输模式，非常适用于对双向带宽

要求不一样的应用，如 Web 浏览、多媒体点播、信息发布等，因此适用于 Internet 接入、VOD（视频点播）系统等。例如：住宅用户主要是对下载信息感兴趣，所以对他们来说，非对称数字用户线(ADSL)是有效的传输手段。

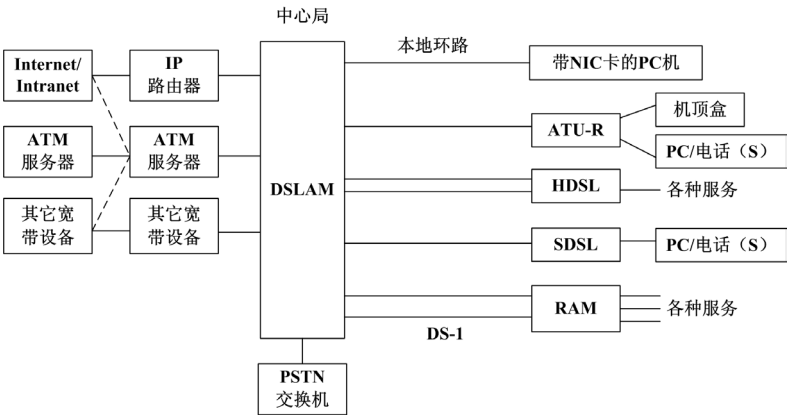
xDSL 技术之间的区别主要体现在信号传输速率和距离的不同以及上行速率和下行速率对称性的不同这两个方面。

3.2.2 DSLAM

DSLAM（DSL Access Multiplexer，DSL 接入复用器）是 xDSL 的局端设备，其连接着网络的客户端（DSL）和网络的服务端（Internet、视频服务等），解决了经常发生在网络服务供应商和最终用户间的“最后一公里”的传输瓶颈问题。

DSLAM 的基本结构如下图所示：

图3-1 DSLAM 的基本结构



注意，此结构并不专用于任何一种 DSL 技术，也并非专用于任何特殊服务。这完全依赖于制造商在制造产品时支持什么。在一种最简单的形式中，DSLAM 可能是一个 ADSL 接入节点并且支持 ADSL 链路和通过一台专有的 TCP/IP 路由器的 Internet 接入。

图中不仅显示了 DSLAM 在 ADSL 网络中的中心位置，而且说明了 DSLAM 在服务和线路构造方面的多功能性。DSLAM 的一些作用并不是很明显。

DSLAM 通常位于中心局（CO）。其它互连的可能性在于实际的布局搭配。在一些具竞争性的环境中，DSLAM 由服务提供商而不是由本地端局拥有并操作。在任何情况下，如果必须继续提供模拟话音服务，DSLAM 可以带有与 PSTN 交换机相连的接口。

在客户端，DSLAM 能与任何一种 DSL 技术和回路相配置。本地回路将终止于一台 PC 机的 ADSL 的网络接口卡（NIC，在这里 ATU-R 是内置的），或者是一台单独包装的用于许多 ADSL 设备（但最初可能只有一个）的 ATU-R。带有一对缆线的 HDSL 能支持多种设备。然而，这将要求在房屋中一个 T1 或 E1 适配接口。SDSL 也能和 ADSL 相同的方式被支持，甚至在一些有 POTS 的情况下。尽管 ISDL 没有在图中显示出来，它也是 DSLAM 所支持的一种 xDSL 技术。Bellcore 已经定义了一种远端接入复用器（RAM）的配置，这种配置为小公司在一对缆线上提供 DS-1 的支持。DSLAM 将支持一种或所有这些 xDSL 技术。然而，必须注意在 DSLAM 中 T1/E1 单元是极其少见的。

在图中的服务端，DSLAM 可以支持 IP 路由器、ATM 交换机，或其它接入服务的宽带设备，诸如 SDV 服务器（也可以接入 ATM 网络中）等等。再强调一次，DSLAM 将提供一种或所有服务的支持。通常，IP 路由用于 Internet 或一个团体的 Intranet 网的接入。作为选择，DSLAM 结构容许通过一个 ATM 交换网络接入所有的服务器和服务。典型地，在 DSLAM 网络服务端的接口是一个 10Base-T 局域网接口。

请认识到基本的 DSLAM 不是一个交换机或路由器，它更象一种类型的复用器。简而言之，DSLAM 复合来自家庭和小办公室的上行信道的比特流并分离来自 IP 或 ATM 的下行信道的庞大的比特流。DSLAM 象一个复用器常做的那样基于信道中的总流量分解这些比特流。所以，从 DSLAM 到其它一些设备的链路，不论它是什么，都必须能够传送突然来自用户的总流量。

3.2.3 IP DSLAM

目前对于 IP DSLAM 的定义众说纷纭，广义的说法是将所有具有 IP 上联端口的 DSLAM 都统称为 IP DSLAM。当然，更准确地说，IP DSLAM 应该称为 Packet DSLAM，这是因为目前许多提供 IP 上联接口的 DSLAM 只完成 Ethernet 层功能，并不对 IP 层协议进行处理。而那些能够完成 IP 层处理，实现 IP 数据包路由的 DSLAM 才是真正意义上的 IP DSLAM。

IP DSLAM 从实现的功能角度划分，可分为两种形态：一种形态的 DSLAM 仅对 Ethernet 层进行处理，另一种形态的 DSLAM 不仅对 Ethernet 层进行处理，而且还对 IP 层进行处理并将宽带接入服务器 BAS 功能集成进来。

第一种形态的 DSLAM 具体完成以下功能：

- 支持二层 Ethernet 数据包的本地转发使能/禁止控制；
- 支持基于端口的二层 Ethernet 数据包的过滤，有些设备还支持基于 MAC 地址（包括源 MAC 地址、目的 MAC 地址）的数据包过滤；

- 支持不同 ADSL 端口的二层隔离；
- 支持 IEEE 802.1Q 协议，支持按照端口划分 VLAN，有些设备还支持按照 MAC 地址划分 VLAN；
- 广播风暴抑制，可对广播包、多播包进行流量抑制；
- 端口配置、端口状态查询和设置，基于端口的数据流收发统计；
- 当 DSLAM 提供多个 FE/GE 上联口时，支持 IEEE802.3ad 链路聚集功能；
- 支持流量控制功能；
- 支持 IGMP Snooping 组播功能。

另外，还有一些设备实现了 IEEE802.1p 优先级控制、IEEE802.1d 生成树功能以及 802.1x 端口接入控制功能。

第二种形态的 DSLAM 除支持 Ethernet 层功能之外，还具备以下功能。

- IP 数据包的转发，支持静态路由、RIPv2、OSPF 协议；
- 支持 IP 组播，并支持 IP 组播 IGMPv2、DVMRP、PIM 协议；
- 支持用户接入速率控制；
- 支持 IP 优先级控制及排队策略（WRR、DRR、WFQ、WF2Q 等），有些设备还支持拥塞控制功能；
- 支持动态和静态分配用户 IP 地址；
- 宽带接入服务器功能。目前，主流的宽带接入服务器都支持 PPPoE/PPPoA 用户接入控制，也有一些设备同时支持 PPPoE/PPPoA 和 802.1x 认证。由于集成了 BAS 功能，相应的还具有以下功能。
- 支持 ADSL 专线用户 IP 地址防盗用；
- 支持 ADSL 用户接入帐号和端口捆绑；
- 支持限制 ADSL 同一 PVC 下获取 IP 地址数目；
- 支持本地和 RADIUS 认证方式；
- 必须支持自动检测用户的异常下线，并释放相应的网络资源，停止计费；
- 提供认证成功后的用户按时长和流量的计费信息。

Hammer10000 具有二层和三层处理能力。具体说明详见 Hammer10000 的随机资料。

3.3 网络基本知识

3.3.1 OSI（开放系统互联）参考模型

开放系统互联参考模型（OSI）是为解决不同供应商提供的设备之间的通信问题而提出的。通常情况下，不同厂家开发的网络结构和专用协议是不兼容的，为此国际标准化组织设计了 OSI 模型，将网络层次分为 7 个不同的级别，并为不同级别的数据通信建立了一套规则来解决这些兼容性问题，使来自不同厂家的设备可以互相通信。OSI 模型的层次如下图所示：

图3-2 OSI 模型的层次

7	应用层
6	表示层
5	会话层
4	传输层
3	网络层
2	数据链路层
1	物理层

在该模型中，报文起源于发送信息的计算机的应用层，然后逐步传递到物理层，再通过网络媒介传递到接收计算机的物理层，最后传递到接收机的应用层。OSI 模型各层的说明如下：

第 7 层：应用层，提供网络服务的软件，如文件传输、电子邮件、远程登录等。它在用户程序和网络之间提供接口。

第 6 层：表示层，将传出数据从机器指定的格式转换为一个国际标准格式和将传入数据从国际标准格式转换为机器指定的格式。

第 5 层：会话层，允许建立和终止一个通信路径，确保发送方是可靠的并对建立的一个连接有访问权，协调两个系统之间的通信。

第 4 层：传输层，在发送方和接收方之间提供数据流，并确保数据达到正确的目的地。该层的另一个作用是确保分组以接收方和应用程序能处理的速率发送。在接收方，传输层将分组重新组装成报文，并将其传递到更高层。

第 3 层：网络层，决定分组通过网络时采取的路径。网络层还控制网络接收分组的速率，以避免网络拥塞和能从拥塞中恢复。

第 2 层：数据链路层，提供分组传输、执行错误检测和纠错功能，以确保接收和发

送分组包含相同的信息。

第 1 层：物理层，建立计算机设备和网络之间的物理连接，并提供从一个系统到其它系统的比特传输。

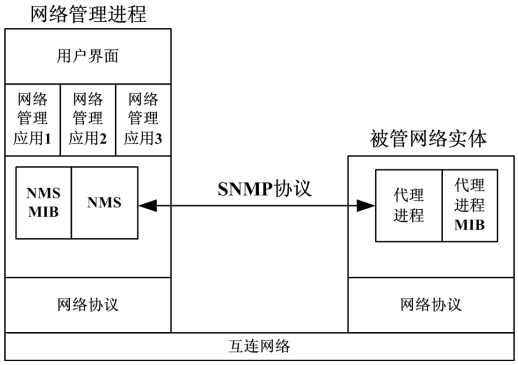
3.3.2 相关网络协议

1. SNMP（简单网络管理协议）

SNMP 是数据网络中使用的最通用的管理协议。它提供了一种从网络设备获得信息并将信息发送到网络设备的手段。SNMP 基于管理员－代理模型，使用管理信息库（MIB）来交换管理员和代理之间的信息。使用 SNMP 协议，管理员通过发送请求到运行在受控设备上的代理来查询和修改每个受控设备的状态和配置信息。所有命令使用 UDP/IP 协议，这意味着管理员和代理之间的通信是无连接的。SNMP 作用于应用层。SNMPV2c 包括 SNMPV1 的基本功能，并增加了新的报文类型、标准化多协议支持、改进的安全性、新 MIB 对象和一种与 SNMPV1 共存方式。SNMPV2c 可用于要使用较少的网络资源来检索大量的管理信息的场合。

SNMP 参考模型如下图所示：

图3-3 SNMP 参考模型



SNMP 参考模型说明了 SNMP 网络管理框架的一般总体结构，以及系统中各个组成部分及其相互关系。其中，主要构成包括：互连网络、网络协议、网络管理进程和被管网络实体。

1） 互连网络

在 SNMP 参考模型中，互连网络是指采用相同协议，通过网关相连的一个或多个网络的集合。如果所实现的全局编址方案正确，采用了标准化的协议，采用的路由

选择方案能保证报文的及时可靠传送，则任意两个端点之间都可以互相通信。

采用 SNMP 时，与此相关的网络协议主要是 TCP/IP。

2） 网络协议

网络协议就是使互连网络能够实现通信的规则。对于采用 TCP/IP 通信的互连网络来说，各种协议分别在组成 TCP/IP 协议集的 4 层协议中运行。举例来说，一台主机会至少在每一层实现一个协议。网络协议常常称为“协议栈”：

- 协议栈中的低层是指最“靠近”硬件的部分。在 TCP/IP 协议集中，这一层称为网络接入层。其主要功能是提供主机与网络间的可靠数据互换。存在很多种网络访问协议，每一种协议都对应于可以连接互连网络上的多种不同类型网络；
- Internet 层负责将数据从源主机传送到目的主机。Internet 层的主要部件是 IP（Internet 协议）。IP 是无连接的数据协议，它并不保证端到端的可靠传输。IP 的特性包括有指定服务类型、Internet 层编址、分片和重组、检验和初步的安全性。Internet 层的另一个重要协议是互连网控制报文协议（ICMP），用来报告差错和拥塞；
- 传输层负责两个进程间的端到端的数据传输，要么用可靠的 TCP，要么用不保证可靠的 UDP；
- TCP/IP 协议栈中的高层网络协议是处理层或应用层。这一层直接为端用户或应用程序提供服务，如 Telnet、FTP、SMTP 和 SNMP 等。

3） 网络管理进程

网络管理进程通过网络协议和 SNMP 协议与互连网络中被管理的网络实体通信，主要包括 4 个部件：

- 网络管理站（NMS）：是监视控制代理进程的处理实体，代理进程在互连网中也是起管理作用的。NMS 及其代理进程形成一个共同体。NMS 可以对每个代理的 MIB 中的特定对象进行读写操作，即管理相应的网络设备。NMS 也可以将每个代理中有关的管理信息存储在自己的本地数据库中；
- 网络管理站的 MIB 和数据库：网络管理站的管理信息库中含有本共同体中所有代理 MIB 的主清单。如果网络管理站要控制每个代理的 MIB 变量，那么它必须知道或能够发现该变量的存在。通常，网络管理站会在其本地数据库中存有自己的 MIB 和额外的管理信息；
- 网络管理应用程序：网络管理应用程序将 SNMP 数据转换成网络管理用户可用的信息。它包括一大堆程序，用于轮询代理、进行 set 和 get 请求，以及处理接收到的陷井报文。网络管理应用程序实现了越来越多非常有用的网络管理功能；

- 网络管理用户界面：端用户是通过用户界面来使用网络管理进程设备的。大多数网络管理进程提供图形用户界面（GUI）来表达性能统计数据、帐务汇总、故障报告、配置清单、创建查询表格、拓扑图等等。

4） 被管网络实体

就是含有代理进程的网络设备。它也要用网络协议和 SNMP 协议在互连网上与网络管理进程的 NMS 通信。被管网络实体包含 2 个关键部件：

- 代理进程：是处理实体，从所在共同体中的 NMS 接收请求，如果请求合法就进行处理，最后发出适当的响应。代理进程也可以配置成要发送陷井报文，以报告异步预定义的事件。代理进程利用操作支持程序操作本地数据结构以提取和设置它所控制的各个 MIB 对象。
- 代理进程的 MIB：代理进程的管理信息库是它所关心的变量集合。构成特定代理管理信息库的 MIB 组决定于该设备的功能和所要管理的资源。

2. TCP/IP（传输控制协议/网际协议）

TCP/IP 是两个使用最广泛的 Internet 协议。

TCP 提供 IP 网络上的数据传输，作用于 OSI 模型的第 4 层，能够向发送方提供到达接收方数据包的传送信息。当传送过程中出现数据包丢失情况时，TCP 可以重新发送丢失的数据包直到数据成功到达接收方或者出现网络超时。TCP 还可以识别重复信息，丢掉不需要的多余信息，使网络环境得到优化。如果发送方传送数据的速度大大快于接收方接收数据的速度，TCP 可以采用数据流控制机制减慢数据的传送速度，协调发送和接收方的数据响应。

IP 作用于 OSI 模型的第 3 层，除了可以提供网络路由之外，还具有错误控制以及网络分段等众多功能。如果 IP 之上的传输设施不可靠（比如 UDP），那么准确数据传输的责任就要上溯到应用层来保障。

TCP/IP 作为一个互连设备和网络的共同起源，广泛用于连接使用不同技术的计算机。大多数管理解决方案需要 TCP/IP 作为信息源和信息载体。

3. UDP（用户数据报协议）

UDP 是一种允许一台机器上的应用程序与另外一台机器上的应用程序交换数据报而不需要确认或保证传递的协议。UDP 作用于 OSI 模型的第 4 层，即传输层。其与 TCP 的明显区别是不具备复杂的可靠性与控制机制。TCP 提供的是面向连接（即在传输前就建立好了点到点的连接）的、可靠的数据流传输，而 UDP 提供的是非

面向连接（即在数据传输前不建立连接，而是在每个中间节点对数据包进行路由）的、不可靠的数据流传输。当强调传输性能而不是传输的完整性时，如音频和多媒体应用，UDP 是一个好的选择。把 SNMP 建立在 UDP 上的部分原因是设计者认为当发生网络阻塞时，UDP 较低的开销使其有更好的机会去传送管理数据；当强调数据传输的完整性、可控制性和可靠性时，则 TCP 是当然的选择。

4. ICMP（Internet 控制报文协议）

ICMP 是伴随 IP 一起必须实现的协议。ICMP 的 RFC 编号是 792。它利用 IP 服务发送各种反映差错和状态的报文。现在有 13 个 ICMP 报文，每个报文的类型值都是唯一的。ICMP 报文及其相应的类型值如下表所示：

表3-1 ICMP 报文类型

报文	类型值
回声（ECHO）回答	0
目的地址不可达	3
源站抑制	4
重定向	5
回声（ECHO）请求	8
超时	11
参数不可理解	12
时间戳请求	13
时间戳回答	14
信息请求	15
信息回答	16
地址掩码请求	17
地址掩码回答	18

ICMP 协议最著名的地方是其在 PING（Packet Internet Groper）程序中的应用。PING 会发出一个类型为回声请求的 ICMP 报文，然后等待回声回答，这样就可以确认在两个端点之间存在 IP 连接。例如，可以用命令：

```
ping 192.168.0.1
```

来测试本机是否可以跟 IP 地址为 192.168.0.1 的设备连接通信。

如果设备连通，将出现以下信息：

```
PING 192.168.0.1 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 192.168.0.1 : bytes=56: icmp_seq=0 ttl=128 time=10 ms
```

```
Reply from 192.168.0.1 : bytes=56: icmp_seq=1 ttl=128 time=5 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=2 ttl=128 time=5 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=3 ttl=128 time=5 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=4 ttl=128 time=5 ms

----192.168.0.1 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 0/36/100
```

如果设备没有连通，将出现以下信息：

```
PING 192.168.0.1 : 56 data bytes.
Press Ctrl-c to Stop.

Request time out.
Request time out.
Request time out.
Request time out.
Request time out.

----192.168.0.1 PING Statistics----
5 packets transmitted, 0 packets received, 100% packet loss
```

3.3.3 网络硬件设备

基本的网络通信设备包括中继器、集线器、网桥、交换机、路由器。这些设备工作在 OSI 模型的不同层，使用不同的网络协议和执行不同的任务。如下表所示：

表3-2 工作在 OSI 模型不同层上的放设备

OSI 模型的层次		该层上的协议	该层上的硬件设备
7	应用层	SNMP Berkeley Services ARPA Services	网关
6	表示层		
5	会话层		
4	传输层	TCP UDP	
3	网络层	IP/IPX ICMP ARP/RARP	路由器 交换机
2	数据链路层	IEEE802.X DHCP MAC地址	网桥 交换机

OSI 模型的层次		该层上的协议	该层上的硬件设备
1	物理层	10Base2 10Base5	简单中继器 集线器

1. 网关

网关工作在应用层，可以包含 OSI 模型的所有层。网关是一个计算系统，通过编程可以实现任何复杂的协议转换和协调，如 IP 和 IPX 之间的转换。

2. 路由器

路由器工作在网络层，其作用是连接两个使用不同技术的网络，并提供分组从一个网络传递到另一个网络的智能解决办法，还能在多个集线器和网桥之间转发流量。

3. 网桥

网桥工作在数据链路层，其作用是允许网络可以具有不同的物理信号，但又具有兼容的数据链接寻址模式。在信息从一个网段流向另一个网段时，对于不需要通过骨干网转发的信息，网桥将进行过滤，从而减少骨干局域网上的流量。网桥的通常用法是允许在一个以太局域网上的用户与一个令牌环局域网上的用户相互通信。

4. 交换机

交换机工作在数据链路层，其作用是将数据发送到目的地，该目的地由分组的低层介质访问控制（MAC）地址决定。交换机象网桥那样，对流量进行限制，且不识别网络协议。现在，新的交换设备是多层交换，或路由交换，这种设备工作在第 3 层，通过路由器智能与交换机效率的结合，从而在数据路由时可以以较高的速度进行。

5. 集线器

集线器工作在物理层。集线器只是一个多口中继器，可以用来增加整个网络的大小和在一个单一网段上的节点数量。集线器允许隔离子网错误，且能在不中断整个网络的情况下向一个网段增加节点。

6. 简单中继器

简单中继器工作在物理层，通常用于将两个网段连接成一个大段，或扩展一个已存在的网段。两个网段之间对传递的报文不进行过滤。简单中继器能对数据信号进行加强，因此可以用来扩展传送距离。简单中继器没有内置网络智能，通常严格用于信号传播。

3.4 操作系统

UniWorks DSL Center 系统的 V1.00 版支持多操作系统平台的应用，可运行在 Microsoft Windows2000/XP、HP-UX、Solaris 等多种操作系统。

有关操作系统的知识，请用户参考操作系统随带的文档资料。

3.5 802.1x协议

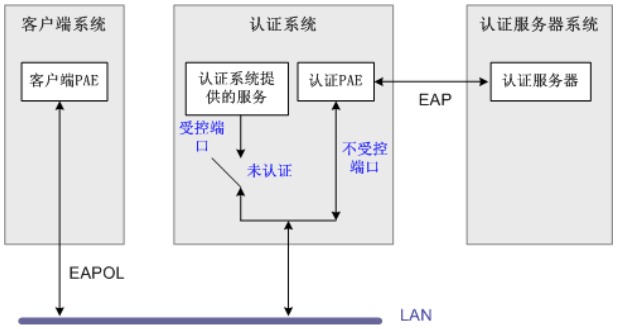
在 IEEE 802 所定义的局域网环境中，只要存在物理的连接口，未经授权的网络设备就可以直接或通过连接到局域网的设备进入局域网络。随着局域网技术的广泛应用，在很多网络环境中，往往不希望未经授权的设备或用户连接到网络，使用网络提供的资源和服务。特别是在运营网络中的应用，对其安全认证的要求已经提到了议事日程上。如何既能够利用局域网技术简单、廉价的组网特点，同时又能够对用户或设备访问网络的合法性提供认证，是目前业界讨论的焦点。IEEE 802.1x 协议正是在这样的背景下提出的。

IEEE 802.1x 称为基于端口的访问控制协议（Port Based Network Access Control Protocol），该协议在利用 IEEE 802 LAN 的优势基础上提供了对连接到局域网的设备或用户进行认证和授权的一种手段。通过此方式的认证，能够在 LAN 这种多点访问环境中提供一种点对点识别用户的方式。这里的端口是指连接到 LAN 的一个单点结构，可以是被认证系统的 MAC 地址，也可以是服务器或网络设备上连接 LAN 的物理端口，或者是在 IEEE 802.11 无线 LAN 环境中定义的工作站和访问点。

3.5.1 802.1x体系结构

IEEE 802.1x 协议的体系结构包括三个重要的组成部分：Supplicant 客户端、Authenticator System 认证系统、Authentication Server 认证服务器。下图描述了三者之间的关系以及相互之间的通信。

图3-4 IEEE 802.1x 认证体系结构



客户端系统一般指用户终端系统，该终端系统通常需要安装一个客户端软件，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。为了支持基于端口的接入控制，客户端系统需支持 EAPOL（Extensible Authentication Protocol Over LAN）协议。

认证系统通常指那些支持 802.1x 协议的网络设备，如港湾网络有限公司的 Hammer 系列交换机和无线访问点设备。支持 802.1x 协议的网络设备对应不同的业务端口（可以是物理端口，也可以是用户设备的 MAC 地址）有两个逻辑端口：受控端口（Controlled Port）和不受控端口（Uncontrolled Port）。不受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可保证客户端始终能够发出或接受认证。受控端口只有在认证通过的状态下才可打开，用于传递网络资源和服务。受控端口可配置为双向受控、仅输入受控两种方式，以适应不同的应用环境。如果用户未通过认证，则受控端口处于未认证状态，用户无法访问认证系统提供的服务。上图中认证系统的受控端口处于未认证状态，因此客户端无法访问认证系统提供的服务。

PAE 是端口访问实体（Port Access Entity），分为客户端 PAE 和认证系统 PAE：

- 客户端 PAE：位于客户端，主要负责响应来自认证系统建立信任关系的请求。
- 认证系统 PAE：位于认证系统，负责与客户端的通信，把从客户端收到的信息传送给认证服务器以完成认证。

认证系统的 PAE 通过不受控端口与客户端 PAE 进行通信，二者之间运行 EAPOL 协议。认证系统的 PAE 与认证服务器之间运行 RADIUS（Remote Authentication Dial In User Service）协议。

认证系统和认证服务器之间的通信可以通过网络进行，也可以使用其他的通信通道。例如当认证系统和认证服务器集成在一起时，两个实体之间的通信就可以不采用 RADIUS 协议。

认证服务器通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用

户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量将接受上述参数的监管。

上图中描述了终端用户的认证机制，对于网络设备之间的认证也是一样。例如：当一个网络设备 A 要求访问网络设备 B 所提供的服务时，系统 A 的 PAE 就成为客户端（Suppliant），系统 B 的 PAE 为认证系统（Authenticator）；如果 B 要求访问 A 所提供的服务时，B 的 PAE 就成为客户端，A 的 PAE 就成为认证系统。

3.5.2 802.1x认证机制

802.1x 作为一种认证协议，在实现的过程中有很多重要的工作机制，这里主要介绍其中的四种机制：

- 认证发起机制
- 退出认证机制
- 重新认证机制
- 认证报文丢失重传机制

1. 认证发起机制

认证过程可以由用户主动发起，也可以由认证系统发起。一方面当认证系统探测到有未经过认证的用户使用网络时，就会主动发起认证；另一方面客户端可以通过客户端软件向认证系统发送 EAPOL-Start 报文发起认证。

- 由认证系统发起的认证

当认证系统检测到有未经认证的用户使用网络时，就会发起认证。在认证开始之前，端口的状态被强制“未认证”。

如果客户端的身份标识不可知，则认证系统会发送 EAP-Request/Identity 报文，请求客户端发送身份标识。这样，就开始了典型的认证过程。

客户端在收到来自认证系统的 EAP-Request/Identity 报文后，将发送 EAP-Response/Identity 报文响应认证系统的请求。

认证系统支持定期的重新认证，可以随时对一个端口发起重新认证的过程。如果端口状态为已认证状态，则当认证系统发起重新认证时，该端口通过认证，状态保持不变；如果未通过认证，则端口的状态改变为未认证状态。

- 由客户端发起认证

如果用户要上网，则可以通过客户端软件向认证系统发送 EAPOL-Start 报文主动发起认证。认证系统在收到客户端发送的 EAPOL-Start 报文后，会发送 EAP-Request/Identity 报文响应用户请求，要求用户发送身份标识，这样就启动了一个认证过程。

2. 退出认证机制

有以下几种方式可以造成认证系统把端口状态从已认证状态改变成未认证状态：

- 客户端未通过认证服务器的认证；
- 管理性的控制端口始终处于未认证状态；
- 与端口对应的 MAC 地址出现故障（管理性禁止或硬件故障）；
- 客户端与认证系统之间的连接失败，造成认证超时；
- 重新认证超时；
- 客户端未响应认证系统发起的认证请求；
- 客户端发送 EAPOL-Logoff 报文，主动下线。

退出已认证状态的直接结果就是导致用户下线，如果用户要继续使用网络则要重新发起一个认证过程。为什么要专门提供一个 EAPOL-Logoff 机制呢？主要是出于如下的安全考虑：当一个用户从一台终端退出后，很可能其他用户不通过发起一个新的认证过程，就可以利用该设备访问网络。提供专门的退出机制，以确保用户与认证系统专有的会话进程被中止，可以防止用户的访问权限被他人盗用。通过发送 EAPOL-Logoff 报文，可以使认证系统将对应的端口状态改变为未认证状态。

3. 重新认证机制

为了保证用户和认证系统之间的链路处于激活状态，而不因为用户端设备发生故障造成异常死机，从而影响对用户计费的准确性，认证系统可以定期发起重新认证过程，该过程对于用户是透明的，即用户无需再次输入用户名和密码。

重新认证由认证系统发起，时间是从最近一次成功认证后算起。交换机上的重新认证功能可以激活或关闭，默认情况下是关闭的。重新认证的时间间隔默认值为 3600 秒（一个小时）。

注意

重新认证的时间设定需要认真的规划，认证系统对端口进入的 MAC 地址的检测能力会影响到该时间的设定。如果对 MAC 地址的检测比较可靠，则重新认证时间可以设长一些。

4. 认证报文丢失重传机制

对于认证系统和客户端之间通信的 EAP 报文，如果发生丢失，由认证系统负责进行报文的重传。在设定重传的时间时，考虑网络的实际环境，通常会认为认证系统和客户端之间报文丢失的几率比较低以及传送延迟低，因此一般通过一个超时计数器来设定，默认重传时间为 30 秒钟。

由于对用户身份合法性的认证最终由认证服务器执行，认证系统和认证服务器之间的报文丢失重传也很重要。

另外注意，对于用户的认证，在执行 802.1x 认证时，只有认证通过后，才能由 DHCP 发起（如果配置为 DHCP 的自动获取）和 IP 地址分配的过程。当客户终端配置了 DHCP 自动获取 IP 地址时，则可能在未启动 802.1x 客户端之前，就发起了 DHCP 的请求，而此时认证系统处于禁止通行状态，这样认证系统会丢掉 DHCP 请求帧。

3.5.3 协议实现内容

802.1x 协议在实现整个安全认证的过程中，其三个关键部分（客户端、认证系统、认证服务器）之间是通过不同的通信协议进行交互的，因此有必要对其相关的通信协议做一介绍。

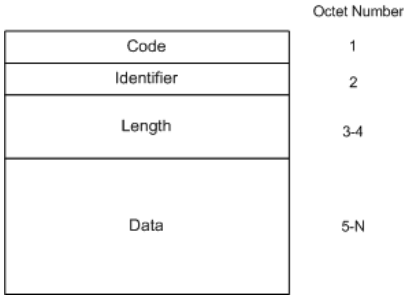
1. EAP 协议

802.1x 协议采用 EAP 协议在客户端、认证系统和认证服务器之间进行通信。EAP（Extensible Authentication Protocol 扩展的认证协议，RFC 2284）是 PPP 认证的一个通用协议，支持多种认证机制。EAP 在链路控制（LCP）阶段并不选择好一种认证机制，而是把这一步推迟到认证阶段，这就允许认证系统在确定某种特定认证机制之前请求更多的信息。

通过支持 EAP 协议，认证系统只需控制其受控端口的状态，而并不干涉通过非受控端口在客户端和认证服务器之间传递的认证信息，这样可实现认证流和业务流的完全分离。可以使用认证服务器来实现各种认证机制，认证系统仅仅需要传送认证信息，并根据认证返回的结果控制受控端口的状态。

EAP 帧结构如下图所示：

图3-5 EAP 帧结构



EAP 帧格式中各字段含义如下表所述：

表3-3 EAP 帧格式中各字段含义

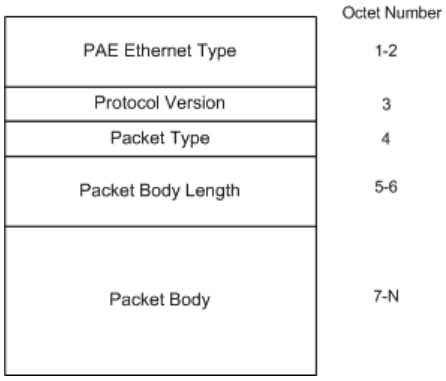
字段	占用字节数	描述
Code	1个字节	表示EAP帧的四种类型： 1．Request 2．Response 3．Success 4．Failure
Identifier	1个字节	用于匹配Request和Response。Identifier的值和系统端口一起单独标识一个认证过程
Length	2个字节	表示EAP帧的总长度
Data	0或更多字节	表示EAP数据

2. EAPOL 协议

802.1x 协议定义了一种报文封装格式，这种报文称为 EAPOL（EAP over LANs 局域网上的扩展认证协议）报文，主要用于在客户端和认证系统之间传送 EAP 协议报文，以允许 EAP 协议报文在 LAN 上传送。

EAPOL 帧结构如下图所示：

图3-6 EAPOL 帧结构



EAPOL 帧格式中各字段含义如下表所述：

表3-4 EAPOL 帧格式中各字段含义

字段	占用字节数	描述
PAE Ethernet Type	2个字节	表示协议类型，802.1x分配的协议类型为888E
Protocol Version	1个字节	表示EAPOL 帧的发送方所支持的协议版本号。本规范使用值为0000 0001
Packet Type	1个字节	表示传送的帧类型，如下几种帧类型： a) EAP-Packet. 值为 0000 0000 ，表示为EAP帧 b) EAPOL-Start.值为0000 0001 ，表示为EAPOL-Start 帧 c) EAPOL-Logoff. 值为0000 0010，表示为EAPOL-Logoff请求帧 d) EAPOL-Key.值为0000 0011 ，表示为EAPOL-Key 帧. e) EAPOL-Encapsulated-ASF-Alert. 值为0000 0100
Packet Body Length	2个字节	表示Packet Body的长度
Packet Body	0或更多字节	如果Packet Type为EAP-Packet、EAPOL-Key或EAPOL-Encapsulated-ASF-Alert的值，则Packet Body取相应的值；对于其他帧类型，该值为空。

EAPOL 帧可以携带 802.1q 的 VLAN 标记。

EAPOL 帧在二层传送时，必须要有目标 MAC 地址，当客户端和认证系统彼此之间不知道发送的目标时，其目标 MAC 地址使用由 802.1x 协议分配的组播地址 01-80-c2-00-00-03。

3.5.4 与不支持802.1x的设备的兼容

对于从一个没有认证的系统过渡到认证系统，最理想的状态是希望能够平滑的进行过渡。由于 802.1x 协议是一个比较新的协议，如果应用在原有的旧网络中，则可能存在与不支持 802.1x 协议的设备的兼容性问题。

如果客户端支持 802.1x 协议，而网络设备不支持（也就是没有认证系统），则客户端是不会收到认证系统响应的 EAP-Request/Identity 报文。在 802.1x 认证发起阶段，客户端首先发送 EAPOL-Start 报文到 802.1x 协议组申请的组播 MAC 地址，以查询网络上可以处理 802.1x 的设备（即认证系统），由于网络中没有设备充当认证系统，所以客户端是得不到响应的。因此客户端在发起多次连接请求无响应后，自动认为已经通过认证。

如果客户端不支持 802.1x 协议，而网络中存在 802.1x 协议的认证系统，则客户端是不会响应认证系统发送的 EAP-Request/Identity 报文，因此端口会始终处于未认证状态。在这种情况下，客户端只能根据协议参数 OperControlledDirections 设定的值通过受控端口访问认证系统，通过未受控端口访问某些通过设置可以访问的服务。

3.6 RADIUS协议

RADIUS 的全称为（Remote Access Dail-In User Service），它是对远程拨号用户访问进行认证的一种协议，是在 RADIUS Server 和 RADIUS Client 之间进行认证、授权、计费的协议标准。认证即辨别用户是谁的过程，通常该过程通过输入有效的用户名和密码实现；授权是指对完成认证过程的用户授予相应权限，解决他能做什么的问题，在一些身份认证的实现中，认证和授权是统一在一起的；计费（Accounting）则是统计用户做过什么的过程，包括用户使用的时间和费用，可通过用户占用系统的时间、接收和发送的信息量来衡量。

RADIUS 采用 Client/Server 模型，在 NAS 上运行的是 Client 端，负责将用户信息传送到指定的 RADIUS 服务器上，并根据服务器返回的结果进行相应的处理。RADIUS 服务器包括两种类型：授权认证服务器和计费服务器。授权认证服务器（RADIUS Authentication Server）负责接收用户的连接请求、验证用户身份，并返回给客户需要的相关配置信息。一个授权认证服务器也可以作为 RADIUS 客户的代理，将其连接到另一个授权认证服务器。计费服务器（RADIUS Accounting Server）负责接受用户计费开始请求和计费结束请求，并实现计费功能。

RADIUS 具有以下属性：

- RADIUS 以 Client/Server 模式工作，实现了对远程用户的身份认证、授权和计费功能。
- RADIUS Client 主要用来将用户信息传递给 RADIUS Server；Server 则对用户进行认证，并返回用户的配置信息。
- 为保证传输的安全性，RADIUS 报文携带由 MD5 算法求得的 128 位验证字。
- 认证具有灵活性。采取多种认证机制，包括 PAP 和 CHAP。

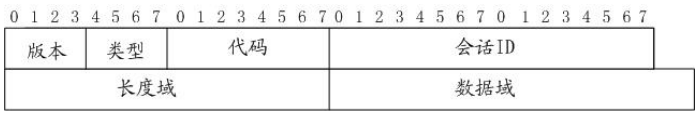
3.7 PPPoE协议

PPPoE（PPP over Ethernet，以太网上点对点协议）是在以太网中传输 PPP 帧信息的技术。它通过把最经济的局域网技术以太网和点对点协议的可扩展性及管理控制功能结合在一起，使网络服务提供商或运营商能够利用可靠和熟悉的技术来加速部署高速互联网业务。它使服务提供商在通过数字用户线、电缆、调制解调器或无线连接等方式，提供支持多用户的宽带接入服务时更加简便易行。同时该技术亦简化了最终用户动态选择这些服务时的操作。

PPPoE 协议共包括两个阶段：发现阶段（PPPoE Discovery Stage）和会话阶段（PPPoE Session Stage）。当一主机希望能够开始一个 PPPoE 会话时，它首先会在广播式的网络上寻找一个宽带接入服务器，当然可能网络上会存在多个宽带接入服务器，对于主机而言则会根据各宽带接入服务器所能提供的服务或用户的预先的一些配置来进行相应的选择。当主机选择完了所需要的宽带接入服务器后，就开始和宽带接入服务器建立一个 PPPoE 会话进程。在这个过程中宽带接入服务器会为每一个 PPPoE 会话分配一个唯一的进程 ID，会话建立起来后就开始了 PPPoE 的会话阶段，在这个阶段中已建立好点对点连接的双方（这种点对点的结构与 PPP 不一样，它是一种逻辑上的点对点关系）就采用 PPP 协议来交换数据报文，从而完成一系列 PPP 的过程，最终将在这点对点的逻辑通道上进行网络层数据报的传送。

PPPoE 的数据报文被封装在以太网帧的数据域内。PPPoE 报文数据域内容会随着会话过程的进行而不断改变。如下图所示：

图3-7 PPPoE 的数据报文格式



其中：

- PPPoE 数据报文最开始的 4 位为版本域，协议中明确规定，这个域的内容是 0x01。
- 类型域占用 4 位，协议中规定，这个域的内容是 0x01。
- 代码域占用 1 个字节，在 PPPoE 的不同阶段，这个域内的内容也是不一样的。
- 会话 ID 占用 2 个字节，在宽带接入服务器还未分配唯一的会话 ID 给用户主机时，该域内的内容必须是 0x0000，一旦主机获取了会话 ID，那么，在后续的所有报文中该域必须填充那个唯一的会话 ID 值。
- 长度域为 2 个字节，用来指示 PPPoE 数据报文中数据的长度。
- 数据域，也称为净载荷域，在 PPPoE 的不同阶段，该域内的数据会有很大不同。在 PPPoE 发现阶段，该域内会填充一些 Tag（标记）；而在 PPPoE 的会话阶段，该域则携带的是 PPP 的报文。

PPPoE 具有如下优点：

- 安装与操作方式类似于以往的拨号网络模式，方便用戶使用。
- 用户处的 xDSL 调制解调器无须任何配置。
- 允许多个用户共享一个高速数据接入链路。适应小型企业和远程办公的要求。
- 终端用户可同时接入多个 ISP，这种动态服务选择的功能可以使 ISP 容易创建和提供新的业务。
- 兼容目前所有的 xDSL Modem 和 DSLAM。
- 可与 ISP 现有接入结构相融合。

4 系统启动

4.1 概述

UniWorks DSL Center 系统启动包括后台服务启动和管理服务器前台启动两部分。管理员必须确定后台服务正在运行后，才能启动 UniWorks DSL Center 系统的管理服务器前台。

4.2 启动后台服务

系统后台服务包括：

- EasyTouch Event Service：事件接收服务，接收设备发过来的日志、告警以及本地操作日志。
- MySql：MySql 数据库，用来存放用户数据

后台服务在 UniWorks DSL Center 系统安装完成后，由后台程序自动在操作系统中注册，并在机器重启后自动启动。而且在每次启动 Windows 时会自动加载该服务，用户不需要手工启动后台服务。

当然，本系统的后台服务也和系统的其它服务一样，用户可以在 Windows 系统的‘开始’－>‘设置’中，或‘我的电脑’中选择‘控制面板’，通过‘管理工具’－>‘服务’快捷键启动 Windows 系统的服务面板。在服务面板中可以找到 UniWorks DSL Center 系统的后台服务名称，用户可以根据需要查看 UniWorks DSL Center 系统后台服务的运行状态、启动类型等属性。请注意不要手工修改这两项服务，如果服务不正常，请重启 Windows 系统或者卸载 UniWorks DSL Center 系统后重新安装。

4.3 启动管理服务器前台

UniWorks DSL Center 系统的管理服务器前台可以通过 Windows 的‘开始’ －

＞‘程序’ －＞‘Dsl Center’－＞‘DSL Center’进行启动，也可以通过在桌面上创建快捷方式进行启动。

4.3.1 登录

UniWorks DSL Center 系统的管理服务器前台启动后，首先会要求用户进行身份验证。用户需输入正确的用户名和密码，然后，点击‘登录’按钮或回车键才能进入并使用系统。

UniWorks DSL Center 系统提供了一个预置用户：

- 用户名：admin，口令：harbour

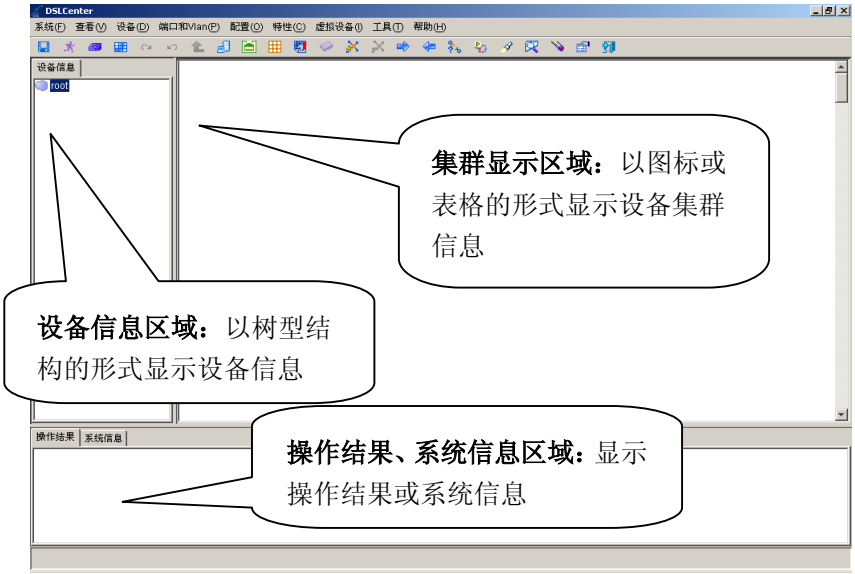
您可以在登录后修改密码，以保证系统安全。具体方法请参见第 8 章“安全管理”的相关内容。

用户如果连续三次登录失败，则此用户名会被锁定（预置用户 admin 不会被锁定）。

4.3.2 前台主界面

用户首次登录时，主界面如下图所示：

图4-1 主界面



UniWorks DSL Center 系统的菜单项说明如下表所述：

表4-1 UniWorks DSL Center 系统的菜单项说明

菜单项	菜单子项		子项功能描述
文件（F）	保存（S）Ctrl-S		保存设备树
	注销（L）Ctrl-D		注销当前用户
	退出（E）Alt-F4		退出UniWorks DSL Center系统。
查看（V）	图标（I）		图标方式显示设备集群信息
	表格（T）		表格方式显示设备集群信息
	前进（P） Ctrl-R		前进到下一视图
	后退（N） Ctrl-N		后退到前一视图
	上一级（U）		回到上一层集群
设备（D）	基本功能（B）	设备信息（D）	查看、配置设备信息
		重启设备（R）	重新启动设备
		保存设备（S）	保存设备当前配置
		擦除设备（E）	擦除设备配置，恢复到出厂状态
		重启业务板(O)	重新启动设备业务板
	设备版本信息（V）		查看设备的版本信息
	配置设备PVC服务（P）		设置vpi和vci
	Slot		查看设备板卡信息
	CPU利用率		查看CPU、内存状态
	Telnet Ctrl-T		Telnet登录设备
端口和VLAN（P）	端口管理（P）Ctrl-P		包括端口状态、认证、绑定和速率配置
	VLAN管理 Ctrl-L		Normal、Super、Sub Vlan配置以及VID使用模式管理

菜单项	菜单子项	子项功能描述
配置（O）	业务配置向导（G）Ctrl-G	指导用户按向导完成设备的业务配置
	在线升级（F）Ctrl-F	升级和保存设备系统、配置文件
	安全管理（U）Ctrl-U	配置登录用户和权限
	事件管理（E）Ctrl-E	日志和告警管理
特性（C）	PPP配置	配置PPP协议
	IP获取方式	配置设备IP获取方式
	802.1x管理	配置802.1x协议
	RADIUS管理	配置RADIUS
	NAS管理	配置NAS
	静态路由（S）	配置静态路由
	访问控制（C）	配置访问控制
	SYSLOG配置	配置SYSLOG参数
	TRAP配置	配置TRAP参数
	二层PPPOE配置	二层透传配置
	广播抑制（B）	广播抑制配置
虚拟设备（V）	添加设备（V）	在集群中添加设备
	修改设备（M）	修改设备名称、描述等
	删除设备（L）	从集群中删除设备
	导出（E）	导出设备树
	导入（I）	导入设备树
工具（T）	Ping	从主机Ping设备
	启动/停止轮询（P）Ctrl-O	轮询设备的状态
	打开/关闭查询窗口（Q）Ctrl-Q	可以在设备树上查询设备
	自动发现设备（A）	发现指定网段内的DSLAM设备
	打开/关闭自动发现窗口（S）Ctrl-A	显示/隐藏自动发现窗口
	选项（O）	配置当前系统的一些参数
帮助（H）	关于（A）	关于系统版权信息及重新认证
	图例（L）	显示设备和端口状态的图例

5 设备管理

5.1 概述

UniWorks DSL Center 系统的设备管理包括设备信息管理、重启和保存设备、CPU 和内存管理、设备版本信息、端口管理和 VLAN 管理等，不仅功能丰富，而且每个功能都提供了批量配置功能，方便用户，节约时间。

5.2 设备信息管理

5.2.1 概述

作为集中管理 DSLAM 设备的应用软件，UniWorks DSL Center 系统为用户提供了强大的设备信息管理功能，包括设备的添加、删除、发现，设备状态的维护，设备信息的导出、导入等。

同时，用户还可以根据设备的逻辑属性，将设备划归不同的管理集群，建立树状的管理层次结构。集群对象作为网管上的逻辑网元，方便了用户对设备进行分类管理。

5.2.2 发现或添加设备

UniWorks DSL Center 系统提供了手动添加设备和自动发现设备的功能，并允许对设备进行轮询，以获取设备当前的连通状态。系统也支持设备信息的导出和导入，实现信息的备份和载入。

1. 工具

为了方便用户的管理、操作，本系统提供了几个有特色的功能，包括 Ping、自动发现设备、查找设备和轮询设备状态等。

(1) Ping 设备

Ping 操作是通过发送 ICMP 报文，获取设备的连通状态。选择菜单项“工具－Ping”，启动 Ping 设备功能。

功能启动后，系统列出当前可以进行 Ping 操作的设备对象。单击“确定”按钮，系统根据用户选择的设备，发送 ICMP 报文，并打印操作结果。

例如，要测试网络中的设备 10.5.4.20 和 10.21.1.151 的连通状态，只要在系统列出的设备列表中选中这两个设备，然后，按“确定”按钮，系统将对这两个设备进行 Ping 操作，并打印测试结果如下所述：

```
Pinging 10.5.4.20 with 32 bytes of data:
Request time out.
Request time out.
Request time out.
Request time out.
Ping statistics for 10.5.4.20:
Packets:  Sent=4, Received=0, Lost=4(100% loss),
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=0ms, Average=0ms

Pinging 10.21.1.151 with 32 bytes of data:
Reply from 10.21.1.151 : bytes=32: time<10ms TTL=128
Reply from 10.21.1.151 : bytes=32: time<10ms TTL=128
Reply from 10.21.1.151 : bytes=32: time<10ms TTL=128
Reply from 10.21.1.151 : bytes=32: time<10ms TTL=128
Ping statistics for 10.21.1.151:
Packets:  Sent=4, Received=0, Lost=0(0% loss),
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=0ms, Average=0ms
```

由此可以看出：设备 10.5.4.20 没有连通，设备 10.21.1.151 处于连通状态。

(2) 启动轮询

选择菜单项“工具－开始轮询”或是单击工具栏按钮 ，启动轮询功能。根据用户在“选项”功能中的配置，轮询功能可以分别对设备进行 Ping 测试和 SNMP 测试，其中，Ping 测试是通过向设备发送 ICMP 报文来判断网络是否连通；SNMP 测试是通过向设备发送 get 请求来判断设备 SNMP 是否启动及网络是否连通。系统将用不同的图标表示轮询结果：

- 如果设备为连通状态，则显示图标 ；
- 如果 Ping 测试不通，显示图标 ；

- 如果 SNMP 测试不通，则显示图标；
- 如果设备状态未知，显示图标。

在“选项”功能中，用户还可以配置轮询操作的时间间隔，单位秒，取值范围为 10 到 65535 秒，默认值为 15 秒。在主界面的“系统信息”选项卡中，可以查看轮询操作过程。

例如，启动轮询功能后，可以在主界面的“系统信息”选项卡中看到如下的轮询操作过程：

开始处理 IP：10.5.4.40…

开始处理 IP：10.5.4.39…

开始处理 IP：10.5.4.38…

… …

处理 IP：10.5.4.49 完毕

处理 IP：10.5.4.62 完毕

处理 IP：10.5.4.46 完毕

轮询结束

提示

1、中间的“… …”，表示此处省略了部分进程的显示；

2、启动轮询功能后，“工具”菜单项中的“开始轮询”将转变为“停止轮询”，用户可通过选择“停止轮询”关闭系统轮询功能；

3、有关菜单项“选项”配置的详细讲述参见本节（6）的内容。

(3) 查找设备

选择菜单项“工具－打开查询窗口”或是单击工具栏按钮，打开“查询”选项卡，可以进行设备信息查询。

UniWorks DSL Center 系统提供了三种查询类型：集群名称、设备 IP 和设备名称，用户可通过点击查询类型项按钮（系统缺省为集群名称），进行查询类型选择。

查询范围的初始设置为根元素、根元素的第一级集群对象子元素和一个“浏览”元素。单击“浏览”选项，显示设备信息树结构。

指定“查询类型”、“查询范围”并输入关键字后，单击“查询”按钮，系统找到满

足条件的第一个对象，并显示在左侧的面板中。单击“继续查找”按钮，系统继续查找下一个满足条件的设备，直到查询结束。

例如，用户可根据查询目的，选定查询类型为“集群名称”，查询范围为根元素“root”，在关键字中输入要查找的集群名称，如 Group1；或者选定查询类型为“设备 IP”，查询范围为根元素的第一级集群对象子元素，如“Group1”，在关键字中输入要查找的设备 IP，如 10.13.2.72；或者选定查询类型为“设备名称”，查询范围为根元素的第一级集群对象子元素，如“Group1”，在关键字中输入要查找的设备名称，如 DSLAM100，然后单击“查询”按钮，系统将开始查询，并显示查询结果信息。

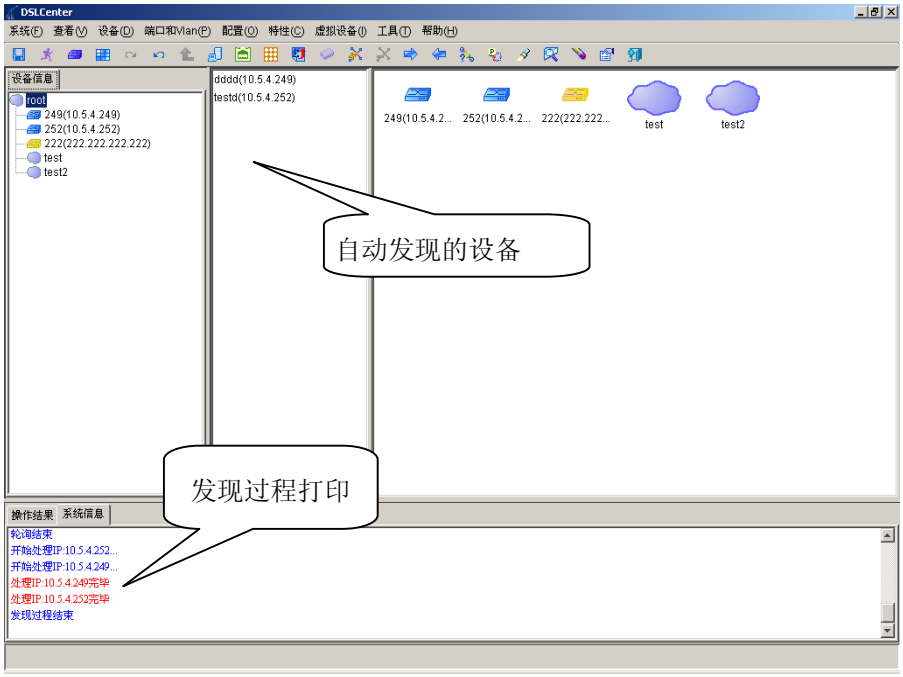
再次单击工具栏按钮 或是选择菜单项“工具－关闭查询窗口”，查询选项卡被关闭。

(4) 自动发现设备

选择菜单项“工具－自动发现设备”或是单击工具栏按钮，启动自动发现设备功能。在弹出的输入框中输入自动发现设备的 IP 地址范围。

系统首先显示发现结果窗口，然后查询在地址范围内的 DSLAM 设备，并获取其连通状态。同时，打印发现过程，如下图所示：

图5-1 自动发现结果



可以将自动发现窗口中的设备拖动到左侧的设备树中。

(5) 打开/关闭自动发现窗口

选择菜单项“工具－打开自动发现窗口”或是单击工具栏按钮，可以重复打开或是关闭自动发现窗口。

(6) 选项

选项功能包括配置检测设备连通，导入、导出设备树信息的默认路径以及模板同步的参数设置。

其中，配置检测设备连通包括：

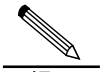
- 设置检测设备是否连通的方式，共包括两种方式：检测是否能 Ping 通设备和检测设备 SNMP 服务是否启动，默认情况下是两种方式都使用。如果设备 SNMP 服务没有启动，则无法管理设备。
- 检查设备是否连通的时间间隔，即每隔多长时间检测一次，默认为 15 秒，取值范围为 10 到 65535 秒。

导入导出设备树配置：

为方便用户，系统提供了导入、导出设备树的默认路径设置，用户可通过“…”按钮进行选择，这样用户每次保存或导入设备树信息时都会出现在默认的路径中。默认为 C:盘根目录。

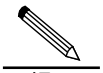
模板同步的参数设置包括两个选项：

- 本地 profile 修改时同步更新设备中的 profile：如果选中此选项，则当本地模板（即 profile）修改时，系统会根据本模板在设备中的存在情况同步更新设备中的 profile，并且，如果有端口已经关联了此 profile，则同时会更新此端口重新关联修改后的 profile；如果没有选中此选项，则修改本地的 profile 模板不会修改设备中的 profile。默认是同步更新设备中的 profile。



建议不要修改本地 profile 模板，如果本地 profile 模板不合适，请另行创建一个合适的 profile 模板。

- 关联时，如果设备中存在同名的 profile，直接关联和修改设备中的 profile 后再关联：在端口关联 profile 时，如果设备中存在同名的 profile，可以有两种选择，直接用此 profile 关联指定的端口，或者用本地的模板修改这个同名的 profile，然后再关联，同时已经和这个 profile 关联的端口也会得到刷新并重新关联。系统默认为直接关联。



建议选择直接关联的方式，这样不会对其他端口造成影响。

2. 虚拟设备

虚拟设备是 UniWorks DSL Center 系统中对设备对象和集群对象的功能抽象。

(1) 添加设备

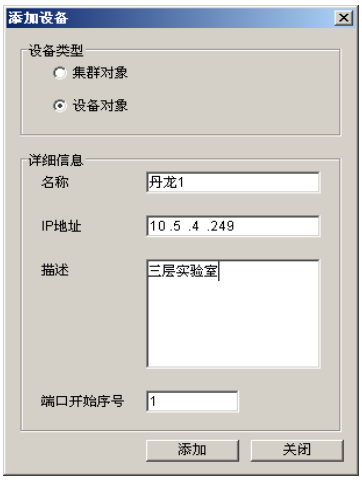
选择一个集群对象，再选择菜单项“虚拟设备－添加设备”或是单击工具栏按钮

，启动添加设备功能。

用户可以添加集群对象或是设备对象。添加设备对象时需要给出具体物理设备的IP地址和端口开始序号，端口开始序号是指该设备的第一个业务端口的编号（对于港湾 Hammer10000 设备第一个业务端口为二槽一端口）。

例如，添加一个设备对象，名称为“丹龙 1”，IP 地址为“10.5.4.249”，描述为“三层实验室”，端口开始序号为“1”，如下图所示：

图5-2 添加设备对象



提示

1、如果要基于设备对象启动添加功能，则提示错误信息：只有集群对象才能添加子设备，请重新选择。

2、系统使用 IP 地址作为设备的标识，因此不能添加重复 IP 地址的设备，否则提示如下信息：要添加的设备已存在，添加失败。

3、端口开始序号是指设备第一个业务端口的编号。

(2) 修改设备

选择一个集群对象或是设备对象，再选择菜单项“虚拟设备－修改设备”，启动设备修改功能。

(3) 删除设备

选择一个集群对象或是设备对象，再选择菜单项“虚拟设备－删除设备”或是单击工具栏按钮，启动删除设备功能。

(4) 导出

系统支持导出 xml 格式的文件。这种格式文件的优点是可以使用 IE 或是任何文本编辑器进行查看和编辑，同时它使用文本形式表达了复杂的层次化结构信息。

选择菜单项“虚拟设备－导出”或是单击工具栏按钮，启动导出功能。

(5) 导入

选择菜单项“虚拟设备－导入”或是单击工具栏按钮，系统将导入选择的 xml 格式的文件。

5.3 图例

通过选择菜单项“帮助－图例”，用户可查看设备连通和端口状态图标所表达的意义，如下图所示：

图5-3 图例

另外，还有：

- 表示具体的设备对象；
- 表示集群对象。

用户了解了图标的意义后，可以直观、方便地判定设备连通或端口状态等信息。

5.4 前进和后退

前进和后退可以让用户方便的回到主面板中的前一视图和后一视图，类似于 Windows 的前进和后退功能。

5.5 设备重新启动

用户可通过选择菜单项“设备－基本功能－重启设备”，在重启设备界面中选中设备后，单击“确定”按钮，系统将重新启动选中的设备，并提示启动进程。

5.6 保存设备

用户可通过选择菜单项“设备－基本功能－保存设备”，在保存设备界面中选中设备后，单击“确定”按钮，系统将启动设备的保存进程。该功能将设备当前的配置信息保存到 Flash 上。

5.7 擦除设备

用户可通过选择菜单项“设备－基本功能－擦除设备”，在擦除设备界面中选中设备后，单击“确定”按钮，系统将启动擦除进程。该功能将删除设备当前的配置信息，将设备恢复到初始状态。

5.8 重启业务板

用户可通过选择菜单项“设备－基本功能－重启业务板”，在重启业务板界面中选中业务板后，单击“确定”按钮，系统将重启选中的业务板。

5.9 设备版本信息

选择一个设备对象或是集群对象，再选择菜单项“设备－设备版本信息”，启动显示设备版本信息功能。

显示设备版本信息的内容包括：设备名称、硬件版本、bootrom 版本、软件版本、制造日期、序列号和 MAC 地址。

5.10 板卡信息管理

选择一个设备对象或是集群对象，再选择菜单项“设备－Slot”，启动显示板卡信息功能。

显示板卡信息的内容包括：设备名称、槽号、槽名称、槽类型、起始端口号、端口数量和序列号。

5.11 CPU利用率

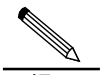
通过选择“设备” －>“CPU 利用率”菜单项，用户可以看到“CPU 管理及内存利用率”信息显示页面，显示用户所选集群中各台设备 CPU 和内存的各项信息，主要内容包括：

- 设备名：设备在集群中的名称
- 设备 IP：设备的 IP 地址
- CPUID：CPU 的标识
- 槽位号：CPU 所在的槽位号
- CPU 主频大小，单位 Hz
- CPU 当前占用率（%）
- CPU 曾达到的最大占用率（%）
- CPU 曾达到的最小占用率（%）
- 总内存，单位 Bytes
- 有效内存，单位 Bytes
- 内存占用率（%）

5.12 Telnet登录

选择一个设备对象，再选择菜单项“设备－Telnet”或是单击工具栏按钮 ，可以启动 Telnet 功能，如果选择多台设备，则登录第一台设备。

5.13 端口管理



Hammer10000 的端口共有三种类型：以太网端口、ADSL 端口和 VDSL 端口。端口的表示方式为 x:y，其中 x 表示槽号，y 表示端口号。

5.13.1 概述

端口管理是交换机中非常重要而且使用比较频繁的管理功能，在本功能模块中集中了端口管理的状态管理、认证管理、绑定管理（IP 绑定管理、MAC 绑定管理、用户名绑定管理）、参数配置管理（以太网端口参数配置、ADSL 端口参数配置、VDSL 端口参数配置）、模板管理（即线路参数管理）以及用户信息管理。

用户只需在端口管理界面中就可完成所有对端口的操作，方便了用户的操作。端口管理主界面如下图所示：

图5-4 端口管理主界面

5.13.2 选择端口

在进入端口管理主界面时，默认是不显示任何端口的信息。当在主界面中选择端口，然后点击鼠标右键进入端口管理，则此时显示选中的端口信息。要配置端口，必须先选择端口。有两种方式可以选择端口：一种是在已选端口输入框中输入端口信息；另一种是点击‘重选端口’按钮进行选择。

1. 在输入框中输入端口信息

在输入框中输入合法的端口字符，然后按回车键或点击‘确定’按钮即可完成重选端口的功能。系统会在选中的每一个设备中搜索符合条件的所有端口进行显示，比如输入 2:1，则会显示每一个选中的设备的 2:1 端口（如果设备上存在的话）。

合法的输入格式为以逗号‘,’分割的端口或端口集合的序列，例如：2:1,3:2-3:5。

如果输入的字符不合法，则提示警告信息：输入的端口无效！正确格式如 1:2,2:4-2:7；如果输入的端口合法，但是没有任何一个设备上有此端口，则会提示

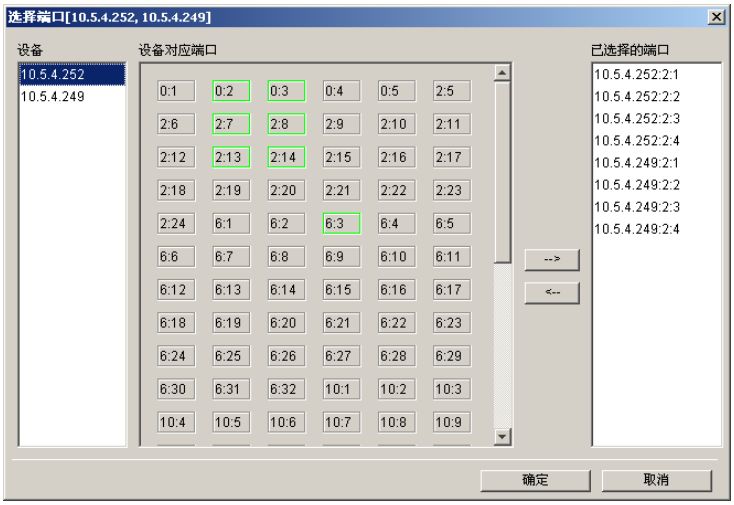
警告信息：无效的端口或端口不存在。

如果输入的端口连续，比如 2:1，2:2，2:3-2:7，则系统会自动简写端口，表示形式为 2:1-2:7。

2. 重选端口按钮选择端口

点击‘重选端口’按钮弹出端口选择对话框，如下图所示：

图5-5 端口选择



在端口选择界面上共分为四部分：

- 设备：列出当前端口管理中选择的所有设备，要选中端口，须先在此选中设备。
- 设备对应端口：列出选中设备的所有端口，供选择。在此区域选择端口时，支持用鼠标单选、连选，如同时按住键盘的“Ctrl”键，则支持复选，选中的端口用绿色框起，如上图所示。
- 选择按钮：‘—>’表示把选中的端口添加到已选择的端口区域；‘<—’表示去除选择。
- 已选择的端口：列出所有已经选择的端口。形如“10.5.4.249:2:1”表示选中的端口是 IP 地址为 10.5.4.249 的设备的 2 槽 1 端口，要想去除选择，则须先在此区域选定端口。

选择好端口后，点击‘确定’按钮即可在端口管理主界面中刷新端口数据。

5.13.3 端口信息

端口信息管理主要是指端口的状态管理。端口共有两个状态参数：管理态参数和运行态参数，共组合成四个状态。其中：

- 管理态：up 或 down。Up 表示此端口已经打开，down 表示此端口已经关闭，此状态可以设置。
- 运行态：up 或 down(或 testing)。Up 表示此端口已经连通，其它则表示端口尚未连通

端口信息的管理共有两个操作：打开端口和关闭端口。选中要操作的端口（可多选），然后点击‘打开端口’或‘关闭端口’即可，成功或失败会有提示。如果部分端口成功部分端口失败，则提示信息会稍微复杂：分别提示每个端口的操作结果，同时端口信息管理界面会刷新数据。

5.13.4 认证管理

端口的认证管理只是针对 xDSL 端口而言的，共有三种认证属性：802.1x、PPPOE 和专线认证（专线认证是指既不采用 802.1x 认证也不采用 PPPOE 认证），认证主界面如下图所示：

图5-6 端口认证

选中要操作的端口（可多选），然后选择右侧的认证方式，点击‘确定’即可，成功或失败会有提示。如果部分端口成功部分端口失败，则提示信息会稍微复杂：分别提示每个端口的操作结果，同时端口认证管理界面会刷新数据。

启动 IP 绑定的端口不能配置 PPPOE 认证。

5.13.5 绑定管理

绑定管理共分为三个功能块：IP 绑定管理、MAC 绑定管理和用户名绑定管理，每个功能块都是独立配置的。

1. IP 绑定

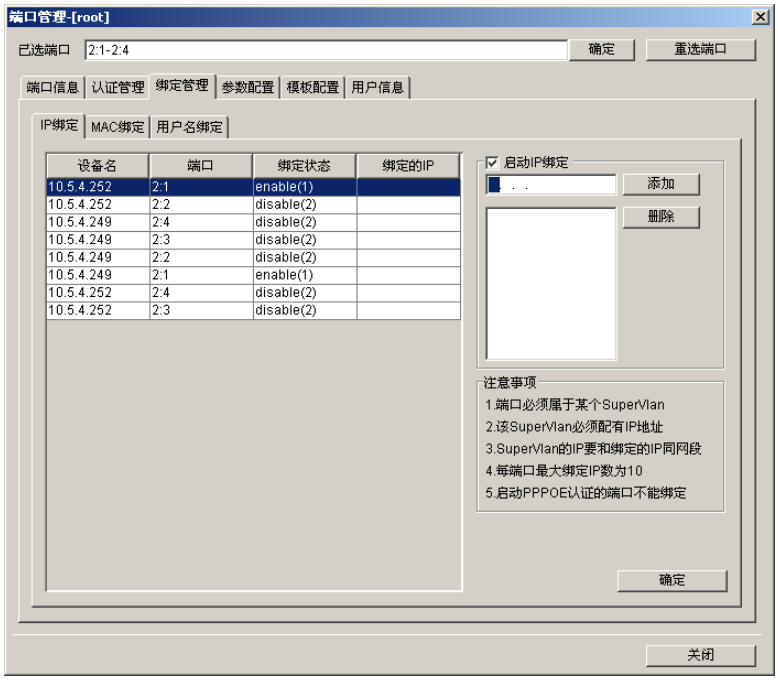
此功能用来限定一个 DSL 端口上只能使用绑定的 IP 地址。如果端口上已经绑定了 MAC 地址，则带此 IP 的 MAC 地址必须是此端口上绑定的 MAC。若使该功能有效，需做以下操作：

1）使能 DSL 端口的 IP 地址绑定

2）在 DSL 端口上绑定 IP 地址

IP 绑定的界面如下图所示：

图5-7 IP 绑定



相关操作如下：

- 首先选中要配置的端口，可以多选；
- 然后选择操作类型，如果是启动 IP 绑定，则在‘启动 IP 绑定’复选框中打钩，如果要禁止 IP 绑定，则不选中‘启动 IP 绑定’；
- 添加或删除 IP：如果是启动 IP 绑定，则添加或删除按钮会使能，否则不能添加或删除 IP 地址。添加 IP 地址的方法是在 IP 输入框中输入 IP 地址，然后点击‘添加’按钮。重复多次，可以添加多个 IP 地址，最多 10 个，当达到能够绑定的最多 IP 地址后再添加 IP 会有提示信息，不让再添加；删除 IP 地址的方法是在 IP 列表框中选中 IP 地址（单选或多选），然后点击‘删除’即可。
- 配置完参数，点击‘确定’按钮之后鼠标会被置于等待状态，直到操作完成，弹出提示信息。根据选中的端口的多少，操作完成时间会有所不同。

注意

1、端口必须属于某个 SuperVlan;
2、该 SuperVlan 必须配有 IP 地址;
3、SuperVlan 的 IP 要和绑定的 IP 同网段;
4、启动 PPPOE 认证的端口不能绑定。

2. MAC 绑定

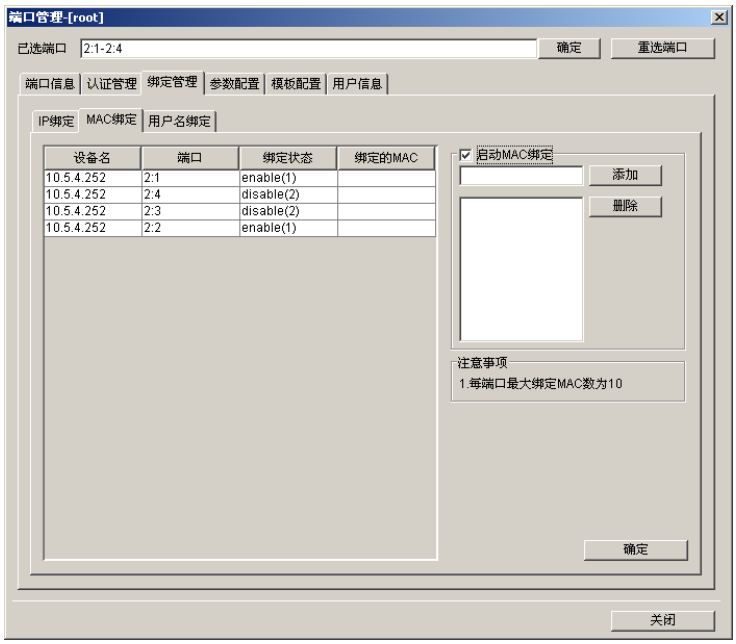
此功能用来限定一个 DSL 端口上只能使用限定的 MAC 地址。若使该命令有效，需作如下操作：

1）使能 DSL 端口的 MAC 地址绑定

2）在 DSL 端口上绑定 MAC 地址

MAC 绑定的界面如下图所示：

图5-8 MAC 绑定



相关操作如下：

- 首先选中要配置的端口，可以多选；
- 然后选择操作类型，如果是启动 MAC 绑定，则在‘启动 MAC 绑定’复选框中打钩；如果要禁止 MAC 绑定，则不选中‘启动 MAC 绑定’。
- 添加或删除 MAC：如果是启动 MAC 绑定，则添加或删除按钮会使能，否则不

能添加或删除 MAC 地址。添加 MAC 地址的方法是在 MAC 地址输入框中输入 MAC 地址，然后点击‘添加’按钮，重复多次，可以添加多个 MAC 地址，最多 10 个，当达到能够绑定的最多 MAC 地址后再添加 MAC 会有提示信息，不让再添加；删除 MAC 地址的方法是在 MAC 列表框中选中 MAC 地址（单选或多选），然后点击‘删除’即可。

- 配置完参数，点击‘确定’按钮之后鼠标会被置于等待状态，直到操作完成，弹出提示信息。根据选中的端口的多少，操作完成时间会有所不同。

提示

在 MAC 地址输入框中正确输入 MAC 地址的方法是连续输入 12 个合法字符（0-9，a-f）。

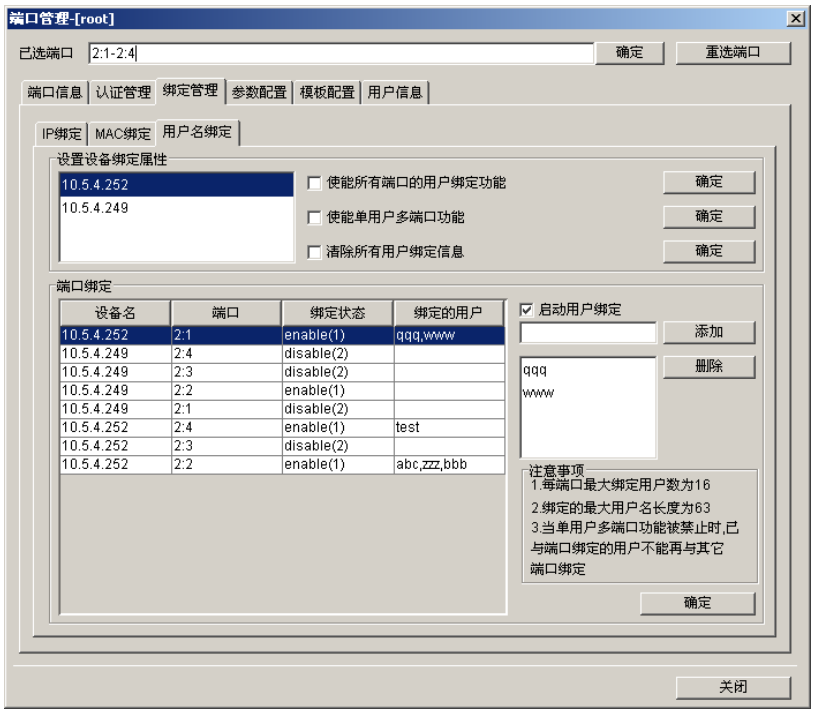
注意

此功能不支持多播 MAC 地址。组成 MAC 地址的 12 个字符中的第二个字符为 1、3、5、7、9、b、d、f 中的任何一个的 MAC 地址就是多播地址。

3. 用户名绑定

如果希望端口只对特定的用户进行认证，可以设置用户绑定功能。每个端口最多可以绑定 16 个用户名。启用该功能后，只有端口上绑定的用户可以进行认证。如果一个用户希望绑定到多个端口，可以打开单用户多端口功能，该功能缺省为禁止状态。用户名绑定界面如下图所示：

图5-9 用户名绑定



用户名绑定功能包括两部分：

- 针对设备的配置
- 针对端口的配置

1）设备绑定属性配置

设备绑定属性共有三个：

- 使能/禁止所有端口的用户绑定功能：选中要操作的设备，选中复选框表示使能，否则表示禁止，然后点击此功能相对应的‘确定’按钮就完成了设置。特别说明的是此操作是针对设备中的所有端口，一旦操作成功，则此设备上的所有业务端口（xDsl 端口）的这个属性都相同。
- 使能/禁止单用户多端口功能：选中要操作的设备，选中复选框表示使能，否则表示禁止，然后点击此功能相对应的‘确定’按钮就完成了设置。一旦使能了此功能，则在此设备上就可以把一个用户绑定到多个端口上了。否则不允许把一个用户绑定到多个端口。
- 清除所有用户绑定信息：选中要操作的设备，然后选中复选框，点击此功能相对应的‘确定’按钮就完成了设置。

注意

一旦这个操作正确完成，则所选择的设备上的每一个端口的用户绑定信息都会被清除。

2）端口绑定属性配置

除了前面介绍的针对整个设备的所有端口的操作外，还可以为每一个端口单独配置。

添加或删除用户：不管端口是否启动了用户绑定功能，都可以预先配置要绑定的用户，然后再启动端口绑定功能。

添加用户的方法是在用户名输入框中输入用户名称，然后点击‘添加’按钮，重复多次，可以添加多个用户名称，最多 16 个，每个用户的用户名称长度为 63 个字符，当达到能够绑定的最多用户后再添加用户会有提示信息，不让再添加；删除用户的方法是在用户列表框中选中用户名称（单选或多选），然后点击‘删除’即可。

配置完参数，点击‘确定’按钮之后鼠标会被置于等待状态，直到操作完成，弹出提示信息。根据选中的端口的多少，操作完成时间会有所不同。

5.13.6 参数配置

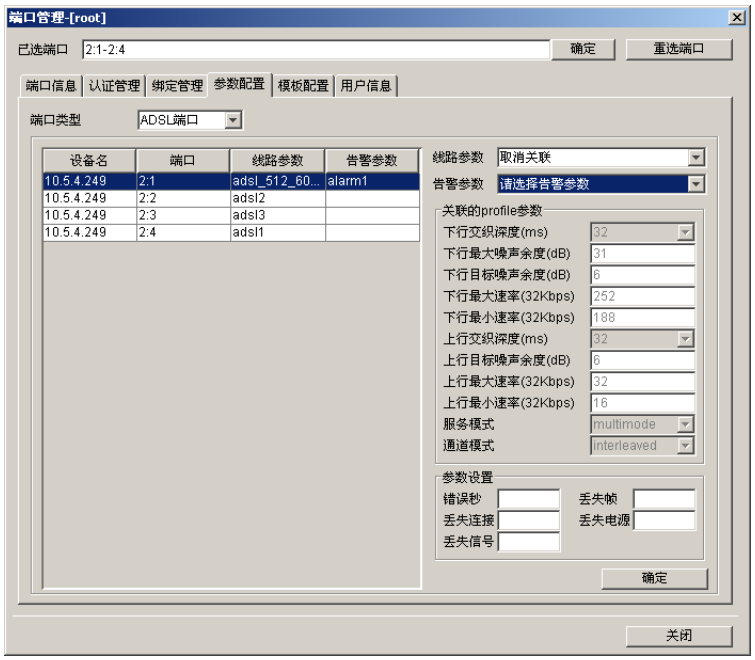
参数配置不仅包括业务端口的配置，同时也包括以太网端口的配置。在对业务端口的配置中，为了方便用户，特创建相应类型的端口配置模板，从而使用户可以利用所创建的端口配置模板对同类型端口直接配置，以简化用户操作，节省时间，提高效率。以太网端口的配置由于配置项少，而且端口也比较少，所以就采用直接配置的方法进行配置。

在用户输入的端口中，系统会根据选定的端口类型自动过滤符合条件的端口：ADSL 端口、VDSL 端口和以太网端口。

1. ADSL 端口参数配置

ADSL 端口的参数配置模板共有两个：线路参数模板和告警参数模板。ADSL 参数配置界面如下图所示：

图5-10 ADSL 参数配置



在 ADSL 参数配置界面中的左侧表中共有四项参数：设备名、端口、线路参数和告警参数。它表明某个设备上的某个端口关联的线路参数和告警参数。如果线路参数或告警参数项没有参数，则表明此端口没有关联相应的参数。

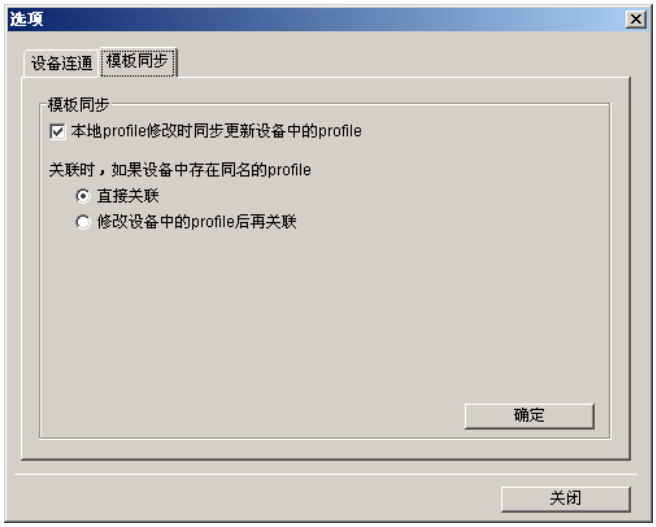
1）模板参数的关联

在线路参数和告警参数选择框中，所有可以选择的参数模板都是本地创建的，当在模板中有模板被选中时，参数模板下面的区域会列出所选模板的各项参数。

选择好合适的模板之后，点击‘确定’按钮等待完成操作。

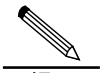
需要说明的是，由于选择的是本地模板，所以可能会存在本地模板和设备上的模板不一致的情况。本系统提供了模板关联选项功能，此选项功能同时也适用于 VDSL 端口，选项界面如下图所示：

图5-11 模板管理选项



选项界面中共提供了两个选项：

- 本地 profile 修改时同步更新设备中的 profile：如果选中此选项，则当本地模板（即 profile）修改时，系统会根据本模板在设备中的存在情况同步更新设备中的 profile，并且，如果有端口已经关联了此 profile，则同时会更新此端口重新关联修改后的 profile；如果没有选中此选项，则修改本地的 profile 模板不会修改设备中的 profile。默认是同步更新设备中的 profile。



建议不要修改本地 profile 模板，如果本地 profile 模板不合适，请另行创建一个合适的 profile 模板。

- 关联时，如果设备中存在同名的 profile，直接关联和修改设备中的 profile 后再关联：在端口关联 profile 时，如果设备中存在同名的 profile，可以有两种选择，直接用此 profile 关联指定的端口，或者用本地的模板修改这个同名的 profile，然后再关联，同时已经和这个 profile 关联的端口也会得到刷新并重新关联。系统默认为直接关联。

建议选择直接关联的方式，这样不会对其他端口造成影响。

2）模板参数的去关联

当有端口已经关联了参数后，如果想去掉此关联，只需选中去关联的端口，然后在模板参数选择框中选择取消关联，点击‘确定’按钮即可。

3）端口关联的 profile 的显示

在 ADSL 端口参数配置界面的左侧表中可以很容易地看到端口关联 profile 的情况。通常情况下，想知道关联的 profile 的具体参数，此时只需在左侧的端口关联表中单击想查看的端口，然后就会在右侧的关联的 profile 区域里显示该 profile 的详细情况。

2. VDSL 端口参数配置

VDSL 端口的参数配置也是通过关联 profile 的形式来配置，配置界面和 ADSL 相似，如下图所示：

图5-12 VDSL 端口配置

在 VDSL 参数配置界面中的左侧表中共有四项参数：设备名、端口、线路参数。它表明某个设备上的某个端口关联的 VDSL 线路参数。如果线路参数项没有参数，则表明此端口没有关联相应的参数。

1）模板参数的关联

在线路参数选择框中，所有可以选择的参数模板都是本地创建的，当在模板中有模

板被选中时，参数模板上面的区域会列出所选模板的各项参数。

选择好合适的模板之后，点击‘确定’按钮等待完成操作。

需要说明的是，由于选择的是本地的模板，所以可能会存在本地模板和设备上的模板不一致的情况，关于参数模板选项的设置请参考 ADSL 参数配置。

2）模板参数的去关联

当有端口已经关联了参数后，如果想去掉此关联，只需选中去关联的端口，然后在模板参数选择框中选择取消关联，点击‘确定’按钮即可。

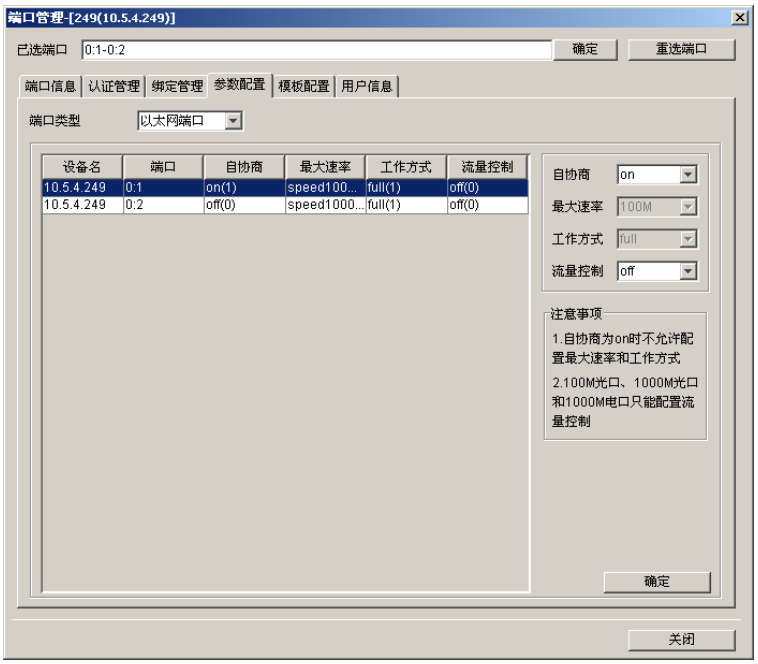
3）端口关联的 profile 的显示

在 VDSL 端口参数配置界面的左侧表中可以很容易地看到端口关联 profile 的情况。通常情况下，想知道关联的 profile 的具体参数，此时只需在左侧的端口关联表中单击想查看的端口，然后就会在右侧的关联的 profile 区域里显示该 profile 的详细情况。

3. 以太网端口参数配置

以太网端口的参数配置包括四个选项：自协商、最大速率、工作方式和流量控制。以太网端口的参数配置界面如下图所示：

图5-13 以太网端口参数配置



选中要配置的端口（可多选），然后设置参数，点击‘确定’即可完成配置操作。

注意

1、只有关闭自协商才能配置最大速率和工作方式;
2、100M 光口、1000M 光口和 1000M 电口只能配置流量控制。

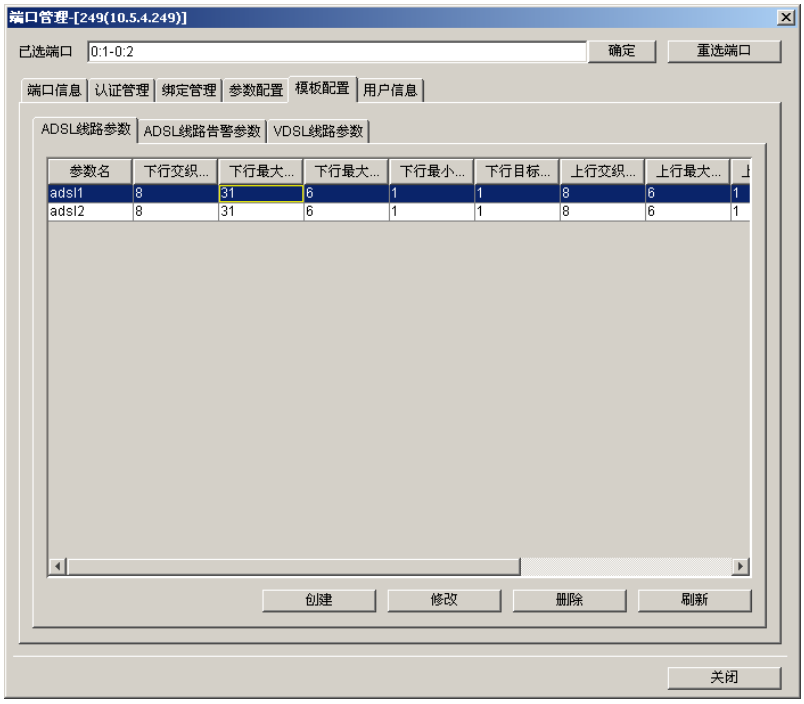
5.13.7 模板配置

为了方便用户配置端口，同时考虑到实际使用的情况，本系统采用配置本地 profile 模板的形式，在实际执行端口关联时再由系统去做各种各样的繁琐操作。这样只要在本地创建几个 profile 模板就可以满足所有需求，不仅使用简单，而且方便。

1. ADSL 线路参数

ADSL 线路模板包括创建、修改和删除。界面如下图所示：

图5-14 ADSL 线路模板参数



1）ADSL 线路参数的创建

在 ADSL 线路模板参数界面中点击‘创建’按钮，弹出 ADSL 模板参数创建界面。

创建 ADSL 线路模板参数只需输入参数名，其它的参数项都有默认值，共有三类参数：下行参数、上行参数以及相应的模式。其中：

下行参数包括：

- 下行交织深度：取值范围为 8、16、32 和 64 中的某一个值，单位为 ms，当通道模式为 fast 时，不用配置此项参数。
- 下行最大噪声余度：通过设置上行/下行数据流的噪声容限可以保证数据的传输质量。取值范围为 0-31，单位为 dB。
- 下行目标噪声余度：通过设置上行/下行数据流的噪声容限可以保证数据的传输质量。取值范围为 0-31，单位为 dB。

注意

最大噪声容限须不小于目标噪声容限。 配置不合适的噪声容限有可能造成链路连接不稳定甚至不能同步。建议采用系统默认值。

下行最大速率：取值范围 1-255。（服务模式为 g.lite 时取值范围为 1-48），单位为 32kbps。所以下行最大速率为 8.160Mbps。

下行最小速率：取值范围 1-255。（服务模式为 g.lite 时取值范围为 1-48），单位为 32kbps。所以下行最大速率为 8.160Mbps。

注意

如果无法建立连接或者连接不稳定，建议适当降低线路速率。

上行参数包括：

- 上行交织深度：取值范围为 8、16、32 和 64 中的某一个值，单位为 ms，当通道模式为 fast 时，不用配置此项参数。
- 上行目标噪声余度：通过设置上行/下行数据流的噪声容限可以保证数据的传输质量。取值范围为 0-31，单位为 dB。

注意

配置不合适的噪声容限有可能造成链路连接不稳定甚至不能同步。建议采用系统默认值。

上行最大速率：取值范围 1-32。（服务模式为 g.lite 时取值范围为 1-16），单位为 32kbps。所以下行最大速率为 1.024Mbps。

上行最小速率：取值范围 1-32。（服务模式为 g.lite 时取值范围为 1-16），单位为 32kbps。所以下行最大速率为 1.024Mbps。

注意 如果无法建立连接或者连接不稳定，建议适当降低线路速率。

模式配置包括：

- 服务模式：ADSL 端口有四种工作模式，包括 multimode、g.lite、g.dmt 和 T1.413，当配置为 g.lite 模式时， 上、下行速率的范围要小得多。
- 通道模式：共两种模式 fast 和 interleaved 。fast 为通道的快速模式，interleaved 为交织模式。快速模式延时低，抗干扰能力差；交织模式延时高，抗干扰能力强。当通道模式为 fast 时不能配置上、下行交织深度。

2）ADSL 线路参数的修改

ADSL 线路参数的修改界面和创建界面一致，只是名称不能修改。

注意 一般情况下，不要修改模板参数。

3）ADSL 线路参数的删除

选中要删除 ADSL 线路模板参数，点击‘删除’即可。一次只能删除一个模板参数。

2. ADSL 告警参数

ADSL 告警模板包括创建、修改和删除。界面如下图所示：

图5-15 ADSL 告警参数模板

1）ADSL 告警参数模板的创建

在 ADSL 告警模板参数界面中点击‘创建’按钮，弹出 ADSL 告警模板参数创建界面。

创建 ADSL 告警模板参数只需输入参数名，其它的参数项都有默认值。系统默认每个参数值为 0。系统在 15 分钟内出现的次数作为它们的门限，0 表示不对该参数设定门限。

2）ADSL 告警参数模板的修改

ADSL 告警参数模板的修改界面和创建界面一致，只是名称不能修改。

注意　一般情况下，不要修改模板参数。

3）ADSL 告警参数模板的删除

选中要删除 ADSL 告警模板参数，点击‘删除’即可。一次只能删除一个模板参

数。

3. VDSL 线路参数

VDSL 线路模板包括创建、修改和删除。界面如下图所示：

图5-16 VDSL 线路参数模板

1）VDSL 线路参数模板的创建

在 VDSL 线路模板参数界面中点击‘创建’按钮，弹出 VDSL 线路模板参数创建界面。

创建 VDSL 线路参数必须输入模板参数名称，其他参数包括下行速率、上行速率、自动协商、流控、双工和最大速率，其中后四项参数和以太网的参数一致。

2）VDSL 线路参数模板的修改

VDSL 线路参数模板的修改界面和创建界面一致，只是名称不能修改。

注意

一般情况下，不要修改模板参数。

3）VDSL 线路参数模板的删除

选中要删除 VDSL 线路模板参数，点击‘删除’即可。一次只能删除一个模板参数。

5.13.8 用户信息

用户信息包括用户名称、联系电话、用户地址、Email 备注信息等。同时还能查看到每个用户的所占用的端口的信息（端口类型、上行速率、下行速率以及端口的认证方式）。

在用户信息中您也可以添加和删除用户信息，导入和导出用户信息以及多种方式查找用户信息。用户信息的界面如下图所示：

图5-17 用户信息管理

1. 添加用户

添加用户的信息包括添加用户名称、用户联系电话以及用户占用的端口等信息。

在添加用户信息界面中输入用户所占用的设备 IP 地址、槽号以及端口号，点击‘显示端口’可以查看如下端口信息：

- 端口类型：ADSL 或 VDSL，如果查不到端口信息则为未知。
- 端口状态：包括管理态和运行态，和端口管理中的端口信息一致。
- 用户名绑定：是否启动了用户名绑定以及绑定的用户名。
- 认证方式：802.1x、PPPOE 或专线，如果查不到端口信息则为未知。
- IP 绑定：是否启动了 IP 绑定以及绑定的 IP 列表。
- MAC 绑定：是否启动了 MAC 绑定以及绑定的 MAC 列表。

输入其他的用户信息（用户名称必须输入，其他项如用户地址、联系电话等可以不输入），然后点击‘确定’，就会在用户信息界面中添加该用户，同时根据输入的端口号取该端口的信息并显示。

2. 修改用户

修改用户信息的主界面和添加用户信息的一样，只是用户名称不能修改。在用户信息的界面中选中要修改的用户（如果选择了多个用户，则只修改第一个用户的信息），点击‘修改用户’，弹出修改对话框，修改数据之后，点击‘确定’完成修改。

3. 删除用户

在用户信息界面中选中要删除的用户（可以多选），然后点击‘删除用户’，系统会弹出确认信息，确认之后，即可删除。

4. 查找用户

由于系统中会存在成千上万的用户信息，要查看一个用户实在不易，因此本系统提供了查找用户的功能，用户可以根据查找条件进行条件查询。查找条件包括所在设备、所在槽号、所在端口号、用户名称、联系电话以及用户的 Email。以上查询条件可以任意组合。查找到的符合条件的用户信息会显示在界面中。

5. 用户信息导出

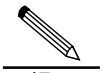
用户信息的数据非常重要，一旦丢失，后果十分严重，所以本系统提供了用户信息

的备份功能。备份文件可以选用 txt 或 excel 的格式，可在点击“导出”按钮后进行选择。

选择好备份格式后，会弹出文件保存对话框，输入文件名称（如果是选择已存在的文件，则系统会提示是否覆盖原文件），完成保存。

6. 用户信息导入

系统也提供了用户信息导入的功能，在导入的时候，采用“追加”的方式导入，即不删除原来的数据，把导入的数据加到已有数据的后面，如果导入的数据用户名称相同，则用导入的数据覆盖原有的数据。导入格式也分 txt 和 excel 两种格式。


提示

在导入数据时，建议保存已有数据。

5.14 VLAN管理

在交换机上设置 VLAN（Virtual Local Area Networks，虚拟局域网）能使网络管理员的配置管理工作变得轻松。这一节主要讲述 VLAN 的相关概念，并说明如何通过 UniWorks DSL Center 系统在交换机上设置 VLAN 的各项属性。

5.14.1 概述

同属一个 VLAN 的所有通信设备看起来好象在同一个物理局域网中。任何一个端口的集合（甚至交换机上的所有端口）都可以被看作是一个 VLAN。VLAN 的划分不受硬件设备物理连接的限制，用户可以通过 UniWorks DSL Center 灵活地划分端口，创建定义 VLAN。

使用 VLAN 具有如下好处：

- VLAN 能帮助控制流量：在传统网络中，不管是否必要，大量广播数据被直接送往所有网络设备，从而导致网络堵塞。而 VLAN 能设置每个 VLAN 中只包含那些必须相互通信的设备，从而减少广播、提高网络效率。
- VLAN 提供更高的安全性：在每个 VLAN 中的设备只能与在同一 VLAN 中的设备通信。例如，如果在市场部的 VLAN *Market* 中的设备必须跟销售部的 VLAN *Sales* 中的设备通信时，就必须通过路由设备才能进行。否则，两个部门就不

能直接通信，从而提高网络安全性能。

- VLAN 使网络设备的变更和移动更加方便：在传统网络中，网络管理员不得不在网络设备的变更和移动上花费大量的时间和精力。如果用户移动到另一个不同的子网，那么每个终端的地址都得重新设置。而使用 VLAN 则不需要这些复杂繁琐的设置。

例如，在 VLAN 网络中，如果市场部 VLAN Market 中的一台终端移动到了另一个网络中的某个端口，若要保留它的原有子网资格，您只需将那个端口设置到 VLAN Market 中就可以了。

注意

每个 VLAN 的名字可以是以字母开头的 1 至 29 个字符组成，这些字符只能是字母、数字或者下划线“_”。空格符、逗号、引号等字符都是不合法的。此外，VLAN 的名字是区分大小写的。

VLAN 的管理共包括四个部分的内容：NormalVlLAN 的管理、SuperVLAN 的管理、SubVLAN 的管理以及 VLAN ID 的使用模式，以下分别介绍。

5.14.2 NormalVLAN管理

NormalVlan 是传统意义上的 VLAN，它可以配置 IP 地址，能且只能包含有 Tag、Untag 的端口。NormalVlan 的管理包括新建、批量创建、配置、删除以及 NormalVlan 的端口隔离功能。NormalVlan 的管理界面如下图所示：

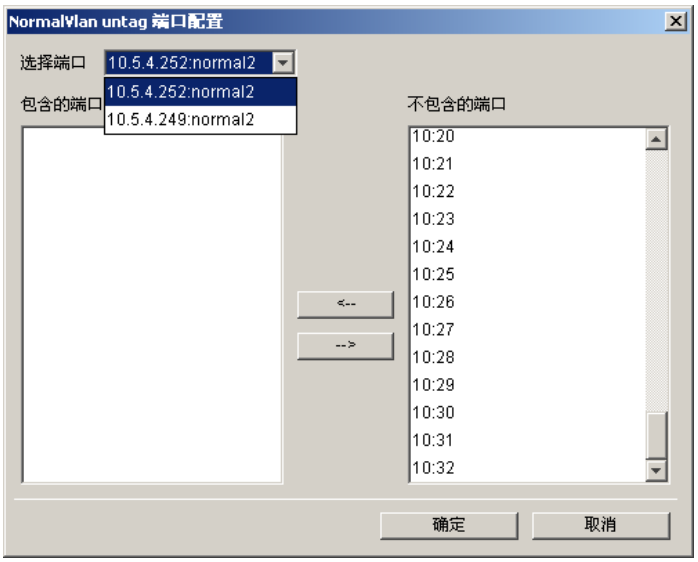
图5-18 NormalVlan 管理

1. 新建 NormalVLAN

默认情况下，在 NormalVLAN 管理界面中，VLAN 信息框中的参数项用来显示已经选中的 Vlan 的信息，且名称和 Vlan ID 是不能编辑的。点击‘新建’按钮之后，Vlan 信息框中的所有内容都被清空，且名称和 Vlan ID 可以编辑。其中：

- VLAN 名称：字母、数字、下划线的组合，VLAN 名称不能相同。
- Vlan ID：1-4095，已经被占用的 ID 不能再被使用。
- IP 地址：在创建 NormalVlan 的时候，IP 地址项参数可选。为了能够支持批量配置，IP 地址不能在 NormalVlan 的管理界面上手工输入，必须点击掩码后面相对应的‘…’按钮，会弹出配置 IP 的界面。由于在创建 Vlan 时，选中的集群中包含两台设备：10.5.4.249 和 10.5.4.252，因此，创建时会在两台设备上分别创建名称为指定名称（此界面中为 normal2）的 Normal Vlan，因此必须为每个 Vlan 配置 IP 地址。在配置 IP 地址界面中输入合适的 IP 地址和掩码后点击‘确定’即可。
- Untag 端口：在创建 NormalVlan 的时候，此项参数可选。并且为了能够支持批量配置，所以 untag 端口不能在 NormalVlan 的管理界面上手工输入，必须点击相对应的‘…’按钮，会弹出配置 untag 的界面如下图所示：

图5-19 配置 untag 端口



配置 untag 端口界面操作共分为四部分：

- 选择端口：在此处选择要配置的 Vlan
- 包含的端口：选中的 Vlan 当前已经包含的端口
- 不包含的端口：选中的 Vlan 不包含的 Vlan，可以添加到选中的 Vlan 中
- 选择和去选择按钮：‘←’表示把选中的‘不包含的端口’添加到‘包含的端口’ 中；‘—>’表示把‘包含的端口’去选择到‘不包含的端口’ 中。显示的‘不包含的端口’都是该 Vlan 所在的设备的实际存在的端口。

可以更替选中的 VLAN 名称来分别单独配置，配置好后，点击‘确定’按钮即可。

- Tag 端口：在创建 NormalVlan 的时候，此项参数可选。并且为了能够支持批量配置，所以 tag 端口不能在 NormalVlan 的管理界面上手工输入，必须点击相对应的‘…’按钮，会弹出配置 tag 的界面。tag 端口的配置和 untag 端口相似，只是可以添加到设备中的 tag 端口只能是以太网端口。

在输入完 VLAN 名称、Vlan ID、IP 地址和掩码（可选）、untag 和 tag 端口（可选）之后，点击 Vlan 信息框中的‘确定’按钮即进行 Vlan 的创建操作。

2. 删除 NormalVLAN

在 Normal Vlan 管理界面中选中要删除的 Vlan（可多选），然后点击‘删除’按钮，完成删除功能。

注意

default vlan 不能删除。

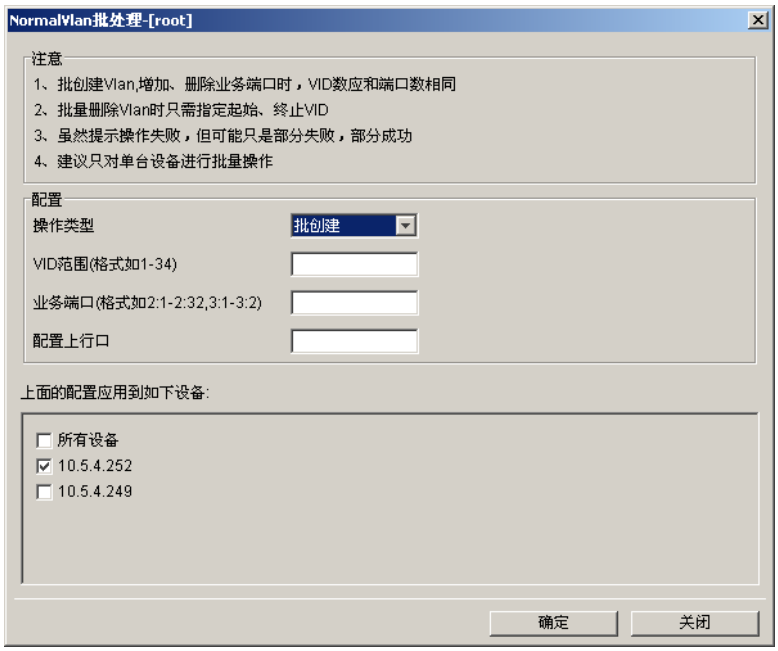
3. 配置 NormalVLAN

配置 NormalVlan 包括配置 IP 地址和配置端口，在 Normal Vlan 管理界面中选中要配置的 Vlan（可多选），然后点击 IP 地址和掩码相对应的‘…’按钮，弹出 IP 配置界面（和创建界面一致），设置好的 IP 地址和掩码会显示在 Normal Vlan 管理界面中；如果要配置 Vlan 的 untag 和 tag 端口，只需做和创建一样的工作即可，最后点击 Vlan 信息框中的‘确定’按钮完成配置。

4. 批处理 NormalVlan

在实际使用中，可能会需要创建许多 Normal Vlan，为了方便用户使用，本系统提供了批量处理 Vlan 的功能，包括批量创建、批量删除、批量配置，批处理 Vlan 界面如下图所示：

图5-20 Normal Vlan 批处理



1）NormalVlan 批创建

在 Normal Vlan 批处理界面中选择‘批创建’，然后输入 VID 范围，格式如 1-34，请确定 VID 是否已经被使用过。

如果在创建时指定业务端口（当然也可以不指定），请按照格式输入，格式如 2:1-2:32，3:1-3:2，并且输入的端口数量一定要和指定的 VID 数相同，否则创建会失败。因为指定的业务端口要一一对应的以 untag 方式加入到指定的 VID 所生成的 Vlan 中。例如指定的业务端口为 2:1-2:10，指定的 VID 范围为 1-10（则生成的 Vlan 为 vlan0001、vlan0002…vlan0010），则端口 2:1 以 untag 方式加入到 vlan0001，端口 2:1 以 untag 方式加入到 vlan0002。

如果在创建时指定上行口（当然也可以不指定），请按照格式输入，格式如 0:1,0:2，所指定的上行口以 tag 方式分别加入到指定的 VID 所生成的 Vlan 中。例如指定的上行口为 0:1,0:2，指定的 VID 范围为 1-10（则生成的 Vlan 为 vlan0001、vlan0002…vlan0010），则端口 0:1 和 0:2 以 tag 方式加入到 vlan0001，同时端口 0:1 和 0:2 以 tag 方式也加入到其他 Vlan（vlan0002…vlan0010）中。

在批处理 Vlan 时，同时也可以指定对多个设备进行操作。由于批处理 Vlan 本身已经很复杂，所以建议一次只针对一台设备操作，除非所有选择的 Vlan 配置都相同而且都比较简单。

配置完参数后，点击‘确定’按钮，开始执行操作，请等待。

创建完成之后，如果要实时查看新创建的结果，请刷新。

2）NormalVlan 批删除

在 Normal Vlan 批处理界面中选择‘批删除’，然后输入要删除的 VID 范围（业务端口和上行口不需输入），然后选择要应用的设备，点击‘确定’按钮即可。

注意

在输入的 VID 范围中，如果有一个 VID 相对应的 Vlan 不存在，则删除失败。

3）NormalVlan 批配置业务端口

批配置业务端口包括批量增加和批量删除。

- 批量增加：在 Normal Vlan 批处理界面中选择‘增加业务端口’，然后输入 VID 范围和业务端口号序列(业务端口数量和VID数量相同,此时上行口不让输入)，再选择此操作应用的设备，点击‘确定’即可。
- 批量删除：在 Normal Vlan 批处理界面中选择‘删除业务端口’，然后输入 VID 范围和业务端口号序列(业务端口数量和VID数量相同,此时上行口不让输入)，再选择此操作应用的设备，点击‘确定’即可。

4）NormalVlan 批配置上行端口

批配置上行端口包括批量增加和批量删除。

- 批量增加：在 Normal Vlan 批处理界面中选择‘增加上行口’，然后输入 VID 范围和上行端口（格式和创建时一致，此时业务端口不让输入），再选择此操作应用的设备，点击‘确定’即可。
- 批量删除：在 Normal Vlan 批处理界面中选择‘删除上行口’，然后输入 VID 范围和上行端口（格式和创建时一致，此时业务端口不让输入），再选择此操作应用的设备，点击‘确定’即可。

5. 刷新

有时可能会出现本地数据和交换机数据不一致的情况（批量操作之后），此时刷新可以取到交换机的最新数据。刷新数据需要一定的时间，请等待。

6. 端口隔离

为了方便用户使用，在 Normal Vlan 管理界面中还提供了一些和 NormalVlan 相关的功能，这样，用户在创建完 Vlan 之后，就可以在同一个界面上完成对 Vlan 的其他配置，无需切换界面。

所谓端口隔离是指板内隔离和板间隔里：

- 板内隔离是指某一个业务板上的端口之间的隔离。业务板上的端口在同属于一个二层 VLAN 的情况下，彼此之间广播报文不能进行互通，实现板内的端口隔离。
- 板间隔离是指分属于不同业务板上的端口之间的隔离。例如端口 2:1 和 3:1，尽管这两个端口属于相同的二层 VLAN，但是同样不能进行广播报文的互通，从而实现不同业务板的端口之间的隔离。

在端口管理界面中，选择要查看的 Vlan（可多选），然后点击‘端口隔离’按钮，弹出端口隔离的界面如下图所示：

图5-21 端口隔离

在端口隔离界面中选择要实行端口隔离的 Vlan，然后点击 ‘使能端口隔离’或‘禁止端口隔离’ 按钮，即可完成操作。

注意

default vlan 不能配置端口隔离。

5.14.3 SuperVLAN管理

随着网络的发展，网络不断膨胀，网络地址资源日趋紧张。由于 B 类地址的匮乏，现在有许多网络不得不用更多的 C 类地址来代替单个的 B 类地址。这虽然解决了一定的问题，但每个子网不得不维护一个路由表，因此造成了资源的更大浪费。于是人们提出了超网的概念（Supernetting），可以使几个高位地址相同的子网共用同一个路由表。

VLAN 聚合的目的是帮助供应商提高 IP 地址的利用率，通过聚合可以使所有在同一子网上的客户（终端用户）通过统一的路由去使用不同的广播域。

给超网（Super VLAN）分配一个子网地址，指定超网的路由地址，其他剩余的地址可以分配给各个主机使用，好像他们只是在同一个大的子网；然后把这个大的子网任意分成若干个“子网”，这些主机的子网掩码完全相同。超网下面只包含子网，不能指定主机。由于各个子网（Sub VLAN）不需要真正的子网网段，有效地提高了 IP 的利用率。这样的子网可以分配足够小，而且可以方便扩展，无需重新定义子网的大小。出于安全目的，可以阻止子网间的相互直接访问，要相互通信需通过路由（因为所有子网的路由都是超网的路由地址）。

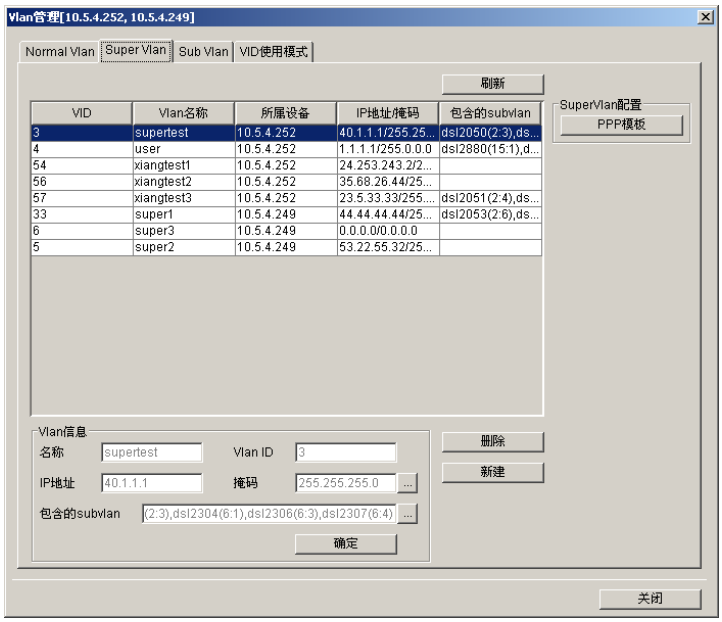
如果不使用聚合的话，每个子网需要设置一个路由地址，而且要分配一个子网地址，结果必然有很多地址被空闲。比如某个网络的总容量只需要 3 个 C 类地址的子网，可能不得不申请使用一个 B 类的地址，而 B 类地址数量又很少，因此会造成地址空间的紧张，浪费资源。

SuperVlan 用于实现 Vlan 的聚合，它具有如下特征：

- 在使用时必须分配一个 IP 地址
- 不能包含端口
- 只能包含 Sub VLAN

SuperVlan 管理界面如下图所示：

图5-22 SuperVlan 管理

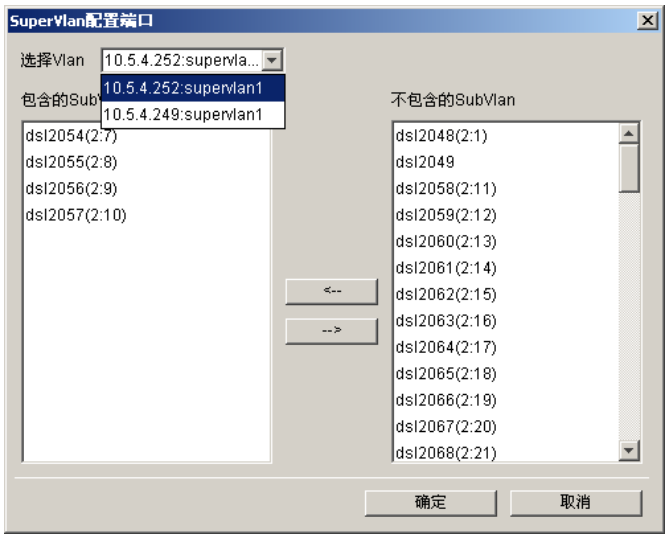


1. 新建 SuperVLAN

默认情况下，在 SuperVlan 管理界面中，Vlan 信息框中的参数项用来显示已经选中的 Vlan 的信息，且名称和 Vlan ID 是不能编辑的。点击‘新建’按钮之后，Vlan 信息框中的所有内容都被清空，且名称和 Vlan ID 可以编辑。其中：

- VLAN 名称：字母、数字、下划线的组合，VLAN 名称不能相同。
- Vlan ID：1-4095，已经被占用的 ID 不能再被使用。
- IP 地址：和创建 NormalVlan 一致
- 包含的 SubVlan：在创建 SuperVlan 的时候，此项参数可选。并且为了能够支持批量配置，所以包含的 SubVlan 不能在此界面上手工输入，必须点击相对应的‘…’按钮，会弹出配置 SubVlan 的界面如下图所示：

图5-23 配置 SuperVlan 包含的 SubVlan



配置 SuperVlan 的 SubVlan 界面操作共分为四部分：

- 选择 Vlan：在此处选择要配置的 Vlan
- 包含的 SubVlan：选中的 Vlan 当前已经包含的 SubVlan
- 不包含的 SubVlan：选中的 Vlan 不包含的 SubVlan，可以添加到选中的 Super Vlan 中
- 选择和去选择按钮：‘←’表示把选中的‘不包含的 SubVlan’添加到‘包含的 SubVlan’ 中；‘—>’表示把‘包含的 SubVlan’去选择到‘不包含的 SubVlan’ 中。显示的‘不包含的 SubVlan’都是该 Vlan 所在的设备实际存在的 SubVlan。

选择方法和 NormalVlan 一致，可以更替选中的 VLAN 名称来分别单独配置，配置好后，点击‘确定’按钮即可。

在输入完 VLAN 名称、Vlan ID、IP 地址和掩码（可选）、包含的 SubVlan（可选）之后，点击 Vlan 信息框中的‘确定’按钮即进行 Vlan 的创建操作。

列出的 SubVlan 名称说明：

dsl2049(2:1)表示端口 2:1 所在的 SubVlan，如果括号里没有列出端口，则说明此 SubVlan 为用户创建的 SubVlan。

2. 删除 SuperVLAN

在 SuperVlan 管理界面中选中要删除的 Vlan（可多选），然后点击‘删除’按钮，完成删除功能。

3. 配置 SuperVLAN

配置 SuperVlan 包括配置 IP 地址和配置包含的 SubVlan。在 Super Vlan 管理界面中选中要配置的 Vlan（可多选），然后点击 IP 地址和掩码相对应的‘…’按钮，弹出 IP 配置界面(和创建界面一致)，设置好的 IP 地址和掩码会显示在 Super Vlan 管理界面中；如果要配置 Vlan 包含的 SubVlan，只需做和创建一样的工作即可，最后点击 Vlan 信息框中的‘确定’按钮完成配置。

4. 刷新

有时可能会出现本地数据和交换机数据不一致的情况，此时刷新可以取到交换机的最新数据。刷新数据需要一定的时间，请等待。

5. PPP 配置

为了方便用户使用，在 SuperVlan 管理界面中还提供了一些和 SuperVlan 相关的功能，这样，用户在创建完 Vlan 之后，就可以在同一个界面上完成对 Vlan 的其他配置，无需切换界面。

选中要配置的 SuperVlan，然后点击‘PPP 配置’，就弹出 PPP 配置界面。关于 PPP 配置，请参见 PPP 配置一节。

注意

只有配置了有效 IP 地址的 SuperVlan 才能配置 PPP。

5.14.4 SubVLAN管理

SubVlan 用于实现 VLAN 聚合。具有如下特征：

- 不能配置 IP 地址
- 能且只能包含有一个端口

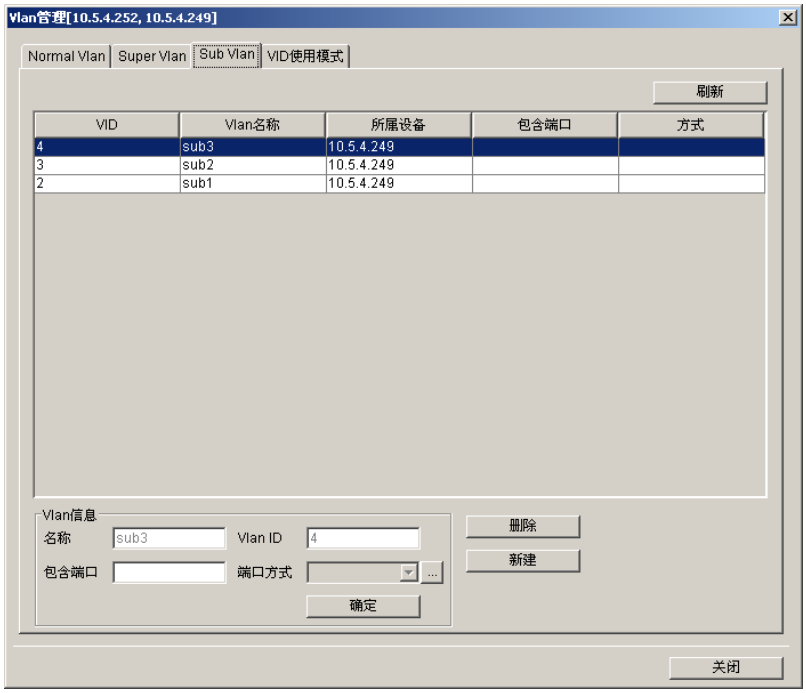
- 只能属于 Super VLAN

对应每一个业务板端口，系统都会自动创建一个 DSL Vlan，即每一个业务板端口都唯一地属于自己的 DSL Vlan，从而实现了业务板端口间的隔离。DSL Vlan 是不可见的，交换机可以通过查看业务板端口来获得对应 DSL Vlan 的信息。DSL Vlan 属于 Sub Vlan 类。但当一个 DSL Vlan 属于一个 Super Vlan 后，该 DSL Vlan 便会出现在 Super Vlan 的 Sub Vlan 列表中。

用户以可以自己创建 SubVlan，并为其配置端口。

SubVlan 管理界面如下图所示：

图5-24 SubVlan 管理



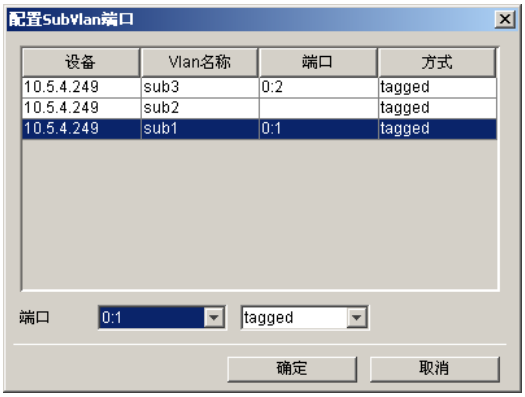
1. 新建 SubVLAN

默认情况下，在 SuperVlan 管理界面中，Vlan 信息框中的参数项用来显示已经选中的 Vlan 的信息，且名称和 Vlan ID 是不能编辑的。点击‘新建’按钮之后，Vlan 信息框中的所有内容都被清空，且名称和 Vlan ID 可以编辑。其中：

- VLAN 名称：字母、数字、下划线的组合，VLAN 名称不能相同。
- Vlan ID：1-4095，已经被占用的 ID 不能再被使用。
- 包含端口：在创建 SubVlan 的时候，此项参数可选。为了能够支持批量配置，

包含的端口不能在此界面上手工输入，必须点击相对应的‘…’按钮，会弹出配置端口的界面，如下图所示：

图5-25 配置 SubVlan 的端口



选中要配置的 SubVlan 名称，然后从界面中选择端口，并且配置该端口加入 SubVlan 的方式，交替选择，为每一个 SubVlan 配置端口。

在输入完 VLAN 名称、Vlan ID、包含的端口（可选）之后，点击 Vlan 信息框中的‘确定’按钮即进行 Vlan 的创建操作。

注意

由于每个业务端口都属于它自己的 SubVlan，所以创建的时候，可以选择的端口只有以太网端口。

2. 删除 SubVLAN

在 SunVlan 管理界面中选中要删除的 Vlan（可多选），然后点击‘删除’按钮，完成删除功能。

3. 配置 SubVLAN

配置 SubVlan 只包括配置端口，在 Sub Vlan 管理界面中选中要配置的 Vlan（可多选），然后点击相对应的‘…’按钮，弹出端口配置界面（和创建界面一致），设置好的端口会显示在 Super Vlan 管理界面中，最后点击 Vlan 信息框中的‘确定’按钮完成配置。

4. 刷新

有时可能会出现本地数据和交换机数据不一致的情况，此时刷新可以取到交换机的最新数据。刷新数据需要一定的时间，请等待。

5.14.5 VID使用模式

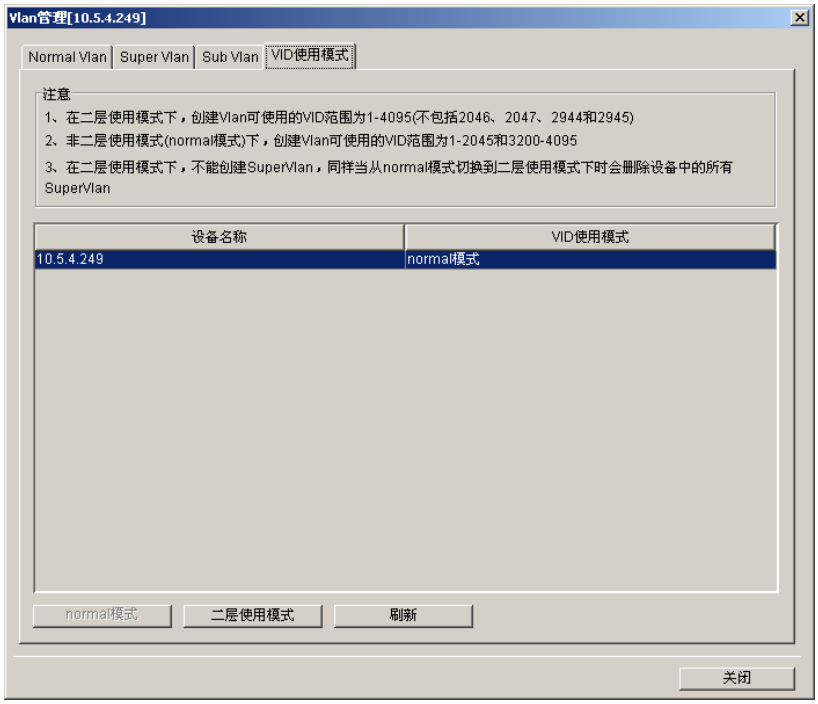
VID 有两种使用模式：二层使用模式和非二层使用模式，系统默认是非二层使用模式。

在二层 VID 使用模式下，创建 VLAN 可指定的 VID 范围是 1-4095(不包括 2046、2047、2944 和 2945)。

在非二层 VID（Normal 模式）使用模式下，创建 VLAN 可指定的 VID 范围是 1-2045 和 3200-4095。

配置 VID 使用模式界面如下图所示：

图5-26 配置 VID 模式



选中要配置的设备（可多选），点击‘normal 模式’或‘二层使用模式’即可完成

配置。

注意

在二层使用模式下，不能创建 SuperVlan，同样当从非二层模式（normal 模式）切换到二层模式后，会删除所选设备的所有 SuperVlan。

5.15 PPP配置

5.15.1 概述

PPP 协议是提供在点到点链路上承载网络层数据包的一种链路层协议。PPP 定义了一整套协议，包括链路控制协议（LCP）、网络层控制协议（NCP）和验证协议（PAP 和 CHAP）。PPP 由于能够提供用户验证、易于扩充和支持同异步而获得较广泛的应用。

PPP 工作流程如下：

1） PPP 在建立链路之前首先进行 LCP 协商，协商内容包括工作方式是 SP 还是 MP、Magic Number、验证方式和最大传输单元等。

2） LCP 协商过后进入 Establish 阶段，此时 LCP 状态为 Opened，表示链路已经建立。

3） 如果配置了验证（远端验证本地或者本地验证远端）就进入 Authenticate 阶段，开始 CHAP 或 PAP 验证。

4） 如果验证失败进入 Terminate 阶段，拆除链路，LCP 状态转为 Down；如果验证成功就进行 NCP 协商，此时 LCP 状态仍为 Opened，而 IPCP 或 IPXCP 的状态机进入初始状态。

5） NCP 协商支持 IPCP 和 IPXCP 协商，IPCP 协商主要包括双方的 IP 地址，IPXCP 协商主要包括双方的网络号和节点号。通过 NCP 协商来选择和配置一个或多个网络层协议。每个选中的网络层协议配置成功后，该网络层协议就可通过这条链路发送报文了。

6） 此链路将一直保持通信，直至有明确的 LCP 或 NCP 帧关闭这条链路，或发生了某些外部事件（例如，用户的干预）。

PPP 验证方式有 CHAP 和 PAP：

PAP 认证是两次握手验证，口令以明文的方式传输，其验证过程如下：

1） 被验证方发送用户名和口令到验证方；
2） 验证方根据用户配置查看是否有此用户以及口令是否正确，然后返回不同的响应。

CHAP 认证是三次握手验证，口令是密文方式的，其验证过程如下：
1） 验证方向被验证方发送一些随机产生的报文(Challenge)；
2） 被验证方用自己的口令字和 MD5 算法对该随机报文进行加密，将生成的密文发回验证方(Response)；
3） 验证方用自己保存的被验证方口令字和 MD5 算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应（Acknowledge or Not Acknowledge）。

选择一个或是多个设备对象，再选择菜单项“特性－PPP 配置”，启动 PPP 配置功能。首先是选择要进行 PPP 配置的 VLAN，如下图所示：

图5-27 选择需要进行 PPP 配置的 VLAN

从列表中选择一个或是多个 VLAN，单击“配置”按钮，进入具体配置界面。主要包括四个部分：LCP 协商参数、NCP 协商参数、认证和其他配置（主要是 IP 地址的获取方式）。

5.15.2 LCP协商参数

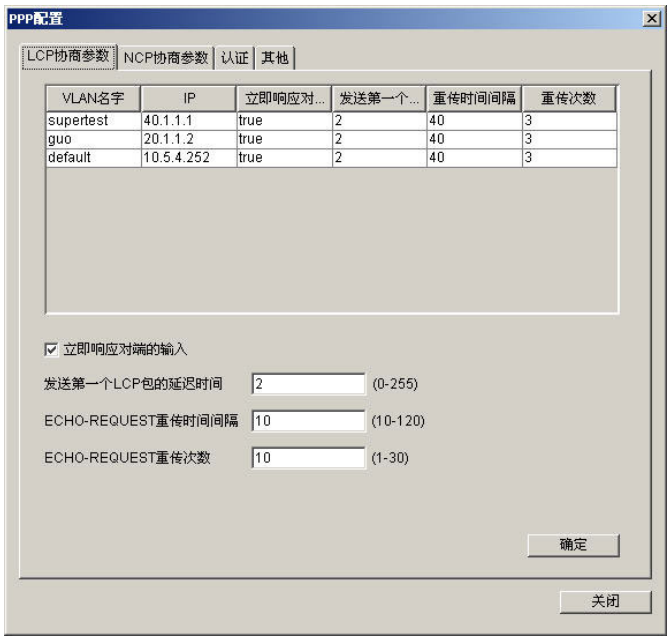
LCP 协商参数配置包括：
- 立即响应对端的输入，配置/取消；
- 发送第一个 LCP 包的延迟时间，单位是秒，取值范围为 0-255，缺省配置为 2

秒；

- ECHO-REQUEST 重传时间间隔，单位是秒，取值范围为 10-120，缺省配置为 10 秒；
- ECHO-REQUEST 重传次数，取值范围为 1-30，缺省配置为 10 次。

系统配置界面如下图所示：

图5-28 LCP 协商参数



选中一个或是多个 VLAN 项，下方参数栏中显示选中 VLAN 的默认参数，修改相关参数，单击“确定”按钮，则配置被下发到设备上，同时更新表中的显示。

5.15.3 NCP协商参数

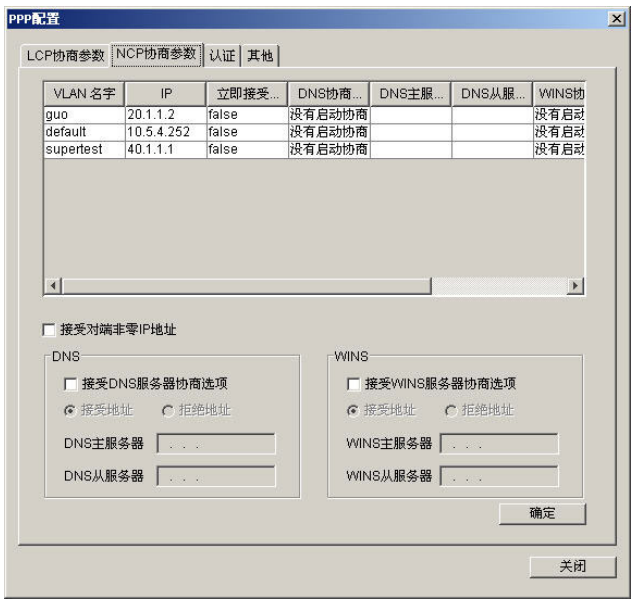
NCP 协商参数配置包括：

- 接受对端非零 IP 地址，配置/取消；
- 接受 DNS 服务器协商选项，配置/取消；
- 接受/拒绝指定的 DNS 服务器；
- 接受 WINS 服务器协商选项，配置/取消；

- 接受/拒绝指定的 WINS 服务器。

系统配置界面如下图所示：

图5-29 NCP 协商参数



选中一个或是多个 VLAN 项，参数栏中显示默认参数值，修改相关参数，单击“确定”按钮，则配置被下发到设备上，同时更新表中的显示。

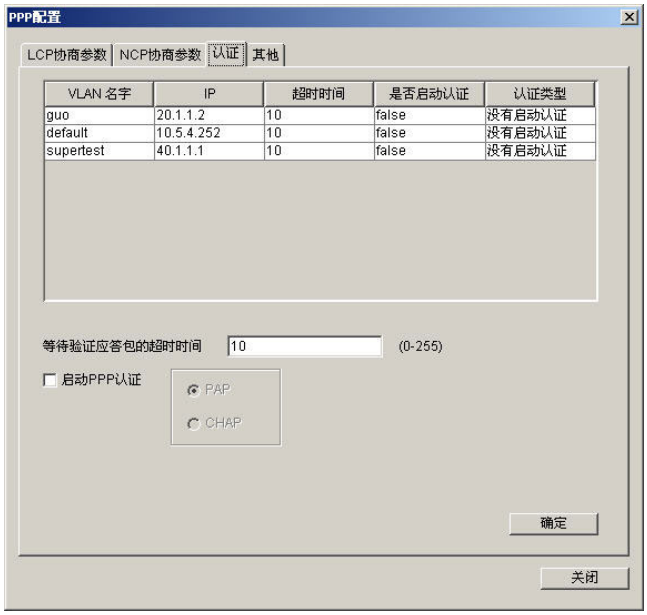
5.15.4 认证

认证协商参数配置包括：

- 等待验证应答包的超时时间，单位是秒，取值范围为 0-255，缺省配置为 10 秒；
- PPP 对对端的验证方式，可选，有 PAP 和 CHAP 两种验证方式。

配置界面如下图所示：

图5-30 认证



选中一个或是多个 VLAN 项，参数栏中显示默认参数值，修改相关参数，单击“确定”按钮，则配置被下发到设备上，同时更新表中的显示。

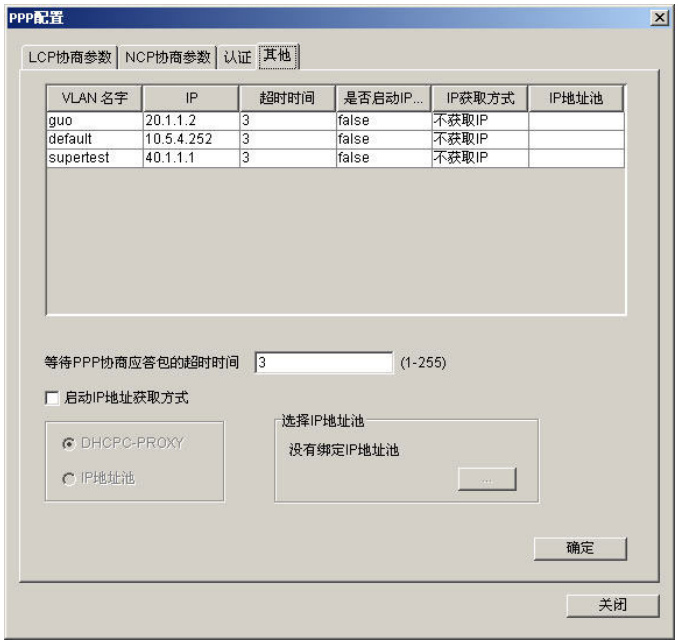
5.15.5 其他配置

其他参数配置包括：

- 等待 PPP 协商应答包的超时时间，单位是秒，取值范围为 1-255，缺省配置为 3 秒；
- IP 地址获取方式，目前本系统支持 IP 地址池和 DHCP Client Proxy 两种方式。

配置界面如下图所示：

图5-31 其他配置



该界面主要进行 IP 地址获取方式的配置。选中一个或是多个 VLAN 项，参数栏中显示默认参数值，修改相关参数，单击“确定”按钮，则配置被下发到设备上，同时更新表中的显示。

如果用户选择使用 IP 地址池方式，则单击按钮 ...，弹出对话框显示设备中包含的所有的本地 IP 地址池。

5.16 IP地址获取方式

5.16.1 概述

通过 DSLAM 设备连接到 Internet 的用户 PC 必须获得 IP 地址后才能真正的访问网络上的各种资源。DSLAM 设备提供了多种获取 IP 地址的方法：IP 地址池、DHCP Client Proxy 等。其中：

- IP 地址池：提供了三种 IP 地址分配方案，即平均分配、指定数目和指定地址范围。
- DHCP Client Proxy：Hammer10000 在 PPPoE 接入的 IP 地址协商阶段，通

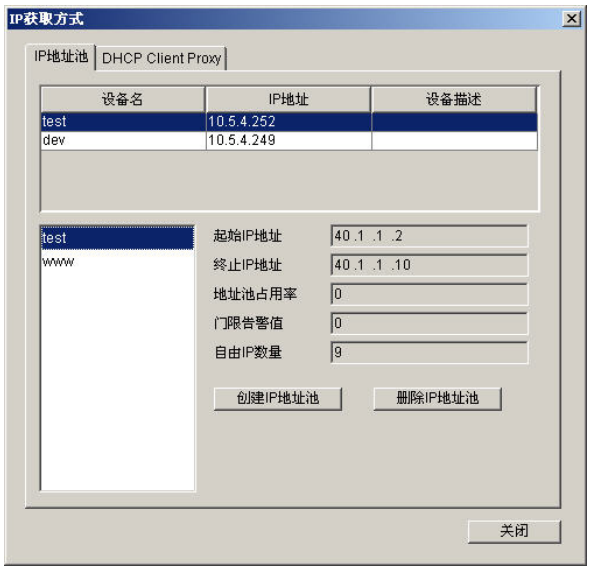
过 DHCP 客户端代理服务向 DHCP 服务器申请地址池中定义的 IP 地址，然后将新申请的 IP 地址返回给客户机，完成 PPPoE 接入的动态分配 IP 地址。当 PPPoE 用户下线时，Hammer10000 发送 DHCP Release 报文通知 DHCP Server 释放 IP 地址。为了保证 DHCP 客户端代理与 DHCP 服务器的正常通信，必须配置一个监听接口。此监听接口必须是与 DHCP 服务器连接通信的上行端口所在的 VLAN，并且必须设置 VLAN 的 IP 地址。

用户可通过选择菜单项“特性—IP 获取方式”配置设备的 IP 地址获取方式。

5.16.2 IP地址池

IP 地址池界面如下图所示：

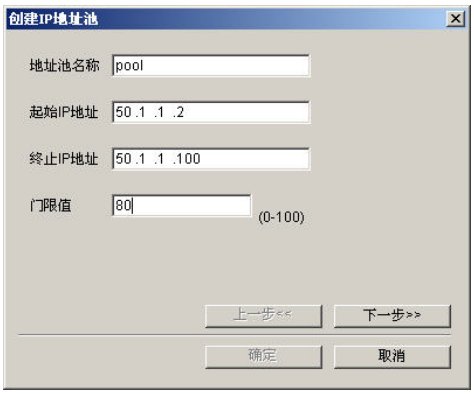
图5-32 IP 地址池



系统显示所选设备的列表，选中一个设备后列出该设备中已经定义的 IP 地址池，选中任一地址池，该地址池的具体参数信息显示在右侧的参数区内，包括起/止 IP 地址、地址池占用率、门限告警值和自由 IP 数量。

单击“创建 IP 地址池”按钮，启动 IP 地址池创建过程，如下图所示：

图5-33 创建 IP 地址池（1）－输入基本信息



输入地址池名称、起/止 IP 地址和门限值，单击“下一步>>”按钮，进入选择设备界面，如下图所示：

图5-34 创建 IP 地址池（2）－选择设备

可以选择要把地址池创建到哪个或是哪几个设备上。单击“下一步>>”按钮，进入地址池分配方案选择界面，如下图所示：

图5-35 创建 IP 地址池（3）－IP 地址池分配方案

系统提供了三种分配方案：

- 平均分配：根据选择的设备，平均分配输入的地址范围，同时提示每个设备被分配的 IP 地址的数目；
- 指定数目：选择设备，在数目域中输入想要分配的 IP 地址的数目，单击“确定”按钮即可；
- 指定地址范围：选择设备，输入起/止 IP 地址，单击“确定”按钮，即给指定设备分配了 IP 地址。

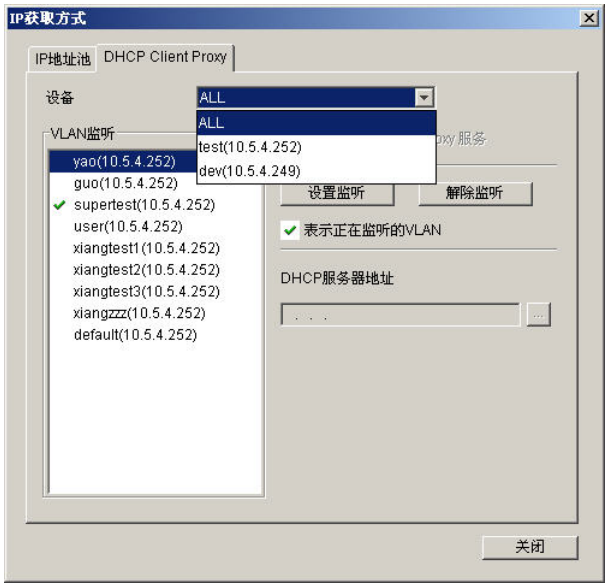
最后按界面下方的“确定”按钮，所有配置下发到设备上。

在创建过程中，用户可以使用“上一步<<”和“下一步>>”按钮，重新选择配置参数。

5.16.3 DHCP Client Proxy

DHCP Client Proxy 配置界面如下图所示：

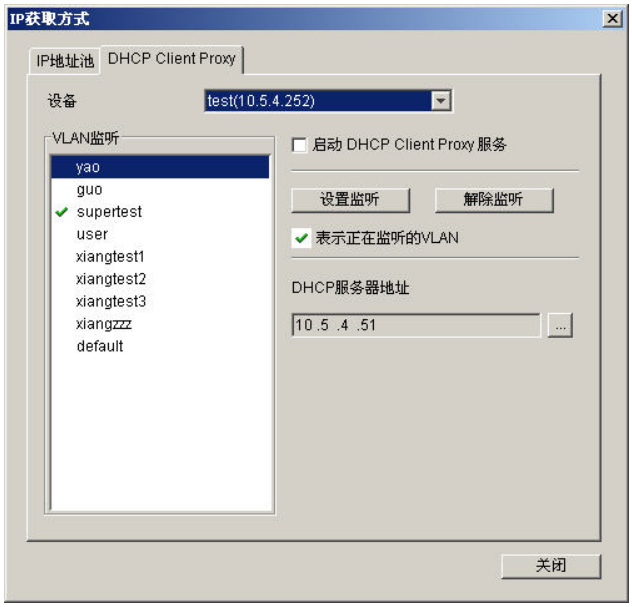
图5-36 DHCP Client Proxy 配置



系统默认选择列出所有选中设备的配有 IP 地址的 VLAN，并显示这些 VLAN 的监听状态。

选择一个设备，如下图所示：

图5-37 某个设备的 DHCP Client Proxy 信息



系统显示属于选中设备的 VLAN 及其监听状态，提示用户当前设备的 DHCP Client Proxy 服务是否启动，显示 DHCP 服务器地址。

用户可以单击“启动 DHCP Client Proxy 服务”复选框，启动或是终止 DHCP Client Proxy 服务。

单击“设置监听”或是“解除监听”按钮，可以切换选中 VLAN 配置监听状态。

用户还可以为该设备指定 DHCP 服务器的地址。

5.17 802.1x管理

5.17.1 概述

802.1x 管理模块共分为六部分：802.1x 管理、协议参数配置、重认证管理、异常下线检测、客户端软件升级以及统计信息查看。

IEEE 802.1x 称为基于端口的访问控制协议（Port based network access control protocol）。IEEE 802.1x 协议的体系结构包括三个重要的部分，即客户端系统（Supplicant System）、认证系统（Authenticator System）和认证服务器（Authentication Server System）：

- 客户端系统：一般为一个用户终端系统，该终端系统通常要安装一个客户端软件，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。为支持基于端口的接入控制，客户端系统需支持 EAPOL（Extensible Authentication Protocol Over LAN）协议。
- 认证系统：通常为支持 802.1x 协议的网络设备。该设备对应于不同用户的端口（可以是物理端口，也可以是用户设备的 MAC 地址、VLAN、IP 等）有两个逻辑端口：受控（Controlled Port）端口和不受控端口（Uncontrolled Port）。不受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可保证客户端始终可以发出或接受认证。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。如果用户未通过认证，则受控端口处于未认证状态，则用户无法访问认证系统提供的服务。
- 认证服务器：通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用户所属的虚拟局域网络（VLAN）、接入带宽、优先级、用户的访问控制列表等等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量就将接受上述参数的监管。

5.17.2 802.1x管理

802.1x 管理模块用于配置 802.1x 相关的各项服务功能以及用户身份验证方式，其中服务功能包括：

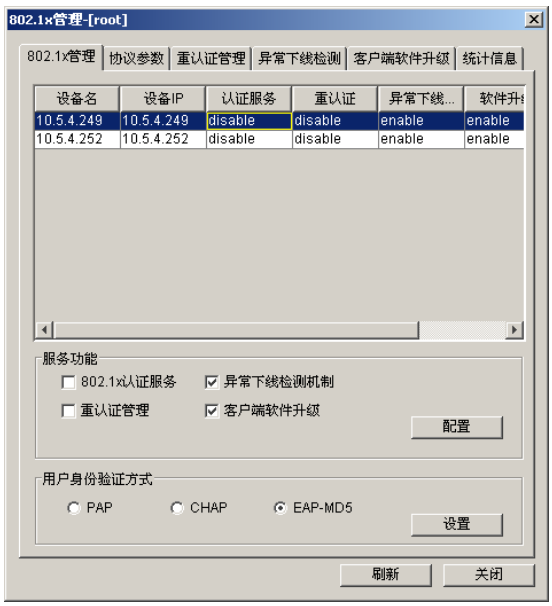
- 802.1x 认证服务，启用/关闭
- 重认证管理，启用/关闭
- 异常下线检测机制，启用/关闭
- 客户端软件升级，启用/关闭

用户身份验证方式包括：

- PAP
- CHAP
- EAP-MD5

用户可通过选择“特性” －>“802.1x 管理” －>“802.1x 管理”菜单项，进入 802.1x 管理界面，如下图所示，并根据实际需要，进行服务功能以及用户身份验证方式的配置。

图5-38 802.1x 管理



查看设备当前配置信息，只需选中要查看的设备，具体配置信息即可在上图下半部分的配置面板上显示出来。

修改设备当前的配置信息，首先需选中欲修改配置的设备（可以单选也可以多选，若选中多台设备则配置面板上将显示所选的第一台设备的当前配置信息），然后，选中欲启用的服务，点击“配置”按钮即可完成 802.1x 相关的各项服务功能配置，选中的服务项将被启用，未选中的服务项则被关闭；设置用户身份验证方式，只需选中欲设定的验证方式，然后点击“设置”按钮即可。

5.17.3 协议参数

用户可通过选择“特性” －>“802.1x 管理” －>“协议参数”菜单项，进入协议参数配置界面，并根据实际需要，进行协议参数的配置，包括：

- 认证失败后不再接受认证的时间间隔：是指在一次认证失败后多长时间内认证系统不接收来自客户端系统的认证请求，这项功能可以防止用户试图不停的进行认证，其取值范围为 0-65535 秒，默认值为 60；
- 重发 EAPOL 数据包的时间间隔：是指认证系统在多长时间内没有收到客户端系统的回复，将会重发 EAPOL 数据包到客户端系统，其取值范围为 1-65535 秒，默认值为 30；
- 接收自客户端系统数据包的超时时间和接收自服务器端数据的超时时间：是用来表示在认证过程中认证系统接收来自客户端系统和认证服务器的数据包的超时时间，其取值范围均为 1-65535 秒，默认值均为 30；
- 认证系统等待回复请求的超时最大次数：是指认证系统等待 supplicants 回复认证请求的超时最大次数，其取值范围为 1-10 次，默认值为 2；
- 允许进行重认证的最大次数：表示端口允许进行重认证的最大次数，其取值范围为 1-10 次，默认值为 2。

5.17.4 重认证管理

为了判断接入的用户是否一直保持连接，有没有因为一些意外情况断掉，NAS（Network Access Server，网络访问服务器）可以定时要求接入的用户进行重认证。

用户可通过选择“特性” －>“802.1x 管理” －>“重认证管理”菜单项，进入重认证管理界面，配置重认证时间间隔，单位秒，默认为 3600 秒，取值范围为 1-65535 秒。

提示

有关 NAS 的讲述参见 5.19 节“NAS 管理”的相关内容。

5.17.5 异常下线检测

异常下线检测用于设置异常下线检测方式及检测时间间隔。异常下线检测机制提供了两种检测方式：

- 设备主动向客户端定期发检测请求：检测周期默认值为 120 秒，取值范围为 10-3600 秒；
- 客户端主动向设备定期发检测请求报文：检测时间间隔默认值为 30 秒，取值范围为 30-600 秒；客户端允许的最大不响应次数默认值为 5 次，取值范围为 2-30 次。

用户可通过选择“特性” －＞“802.1x 管理” －＞“异常下线检测”菜单项，进入异常下线检测配置界面进行相关配置。

5.17.6 客户端软件升级

客户端软件升级用于配置升级客户端软件的网址和升级超时时间。用户可通过选择“特性” －＞“802.1x 管理” －＞“客户端软件升级”菜单项，进入客户端软件升级配置界面进行相关配置。

提示

目前 Hammer10000 仅支持升级网址的配置。

5.17.7 统计信息

802.1x 统计信息包括认证报文统计信息和计费报文统计信息。用户可通过选择“特性” －＞“802.1x 管理” －＞“统计信息” －＞“认证报文统计信息”菜单项，进入认证报文统计信息查看界面，查看认证报文统计信息，包括：

- 1、客户端 EAPOL-START；
- 2、设备端 EAP-REQ/ID；

- 3、客户端 EAP-RESP/ID；
- 4、设备端 ACCESS- RESP/ID；
- 5、Challenge；
- 6、EAP-Req-MD5；
- 7、EAP-Resp-MD5；
- 8、Access-Req-MD5；
- 9、Accept；
- 10、EAP-Success；
- 11、EAPOL-Logoff；
- 12、Reject；
- 13、EAP-Failure。

用户还可以通过单击认证报文统计信息查看界面中的“清除认证报文统计信息”按钮来清除认证统计信息。

用户可通过选择“特性” －＞“802.1x 管理” －＞“统计信息” －＞“计费报文统计信息”菜单项，进入计费报文统计信息查看界面，查看计费报文统计信息，包括：

- 发送开始请求数
- 接收开始请求数
- 发送停止请求数
- 接收停止请求数
- 总发送请求数
- 总接收请求数

5.18 RADIUS管理

5.18.1 概述

RADIUS （Remote Authentication Dial In User Service）远程用户拨号认证系统，是一个在 RADIUS Server 和 RADIUS Client 之间进行认证、授权、配置数据信息交互的协议标准。RADIUS 采用 Client/Server 模型，在 NAS 上运行的是 Client 端，负责传送用户信息到指定的 RADIUS 服务器上，并根据服务器返回的结果进行相应的工作。授权认证服务器（RADIUS Authentication Server）负责接受用户

的连接请求、验证用户身份，并返回给客户需要的相关配置信息。一个授权认证服务器可以作为一个 RADIUS 客户代理连接另一个授权认证服务器。计费服务器（RADIUS Accounting Server）负责接受用户计费开始请求和计费结束请求，实现计费功能。

5.18.2 基本配置

RADIUS 基本配置包括：

- CUT 配置：是否启动 CUT 报文接受功能
- 域配置：包括最大等待消息数以及主备服务器倒换是否通知 NAS
- 认证配置：包括是否启动 RADIUS 认证、是否使能认证服务器倒换功能
- 计费配置：包括是否启动计费功能、重启后是否发送同步报文、是否使能计费服务器倒换功能及超时处理方式

用户可通过选择“特性” －>“RADIUS 管理” －>“基本配置”菜单项，进入 RADIUS 基本配置界面，其中域配置中的“最大等待消息数”只能读取，不提供配置功能。其它配置项可以通过下拉组件框选择指定，设定好之后点击“配置”按钮即可完成配置功能。

5.18.3 认证服务器

用户可通过选择“特性” －>“RADIUS 管理” －>“认证服务器”菜单项，进入 RADIUS 认证服务器的管理界面，如下图所示，进行 RADIUS 认证服务器的创建、查看、修改、删除等操作，中间显示了当前集群中所有的认证服务器。

图5-39 RADIUS 认证服务器管理界面

1. 新建认证服务器

用户可通过选择 RADIUS 认证服务器管理界面中的“创建”按钮，进入新建认证服务器界面。

新建认证服务器时须指定服务器 IP、客户端 IP；UDP 端口可以不指定，默认为 1812，其它配置项包括：

- 共享密钥：认证服务器与 NAS 共享的密钥
- 最大重传数：认证服务器的最大重传数，取值范围为 2-10，默认值为 3 次
- 最大发送失败数：认证服务器的最大发送失败数，取值范围为 2-30，默认值为 5 次
- 服务器状态：RADIUS 认证服务器的状态，只能设置状态为 active
- 重传时间间隔：认证服务器的重传时间间隔，取值范围为 5-300，默认值是 10 秒
- 最大重传丢弃数：认证服务器的最大重传丢弃数，取值范围为 2-30，默认值为 5 次

提示

上述六个配置项可以在创建好之后进行修改。

单击“刷新”按钮可重新设定各个配置项。

用户还可以指定在哪些设备上创建认证服务器，若想在某设备上创建认证服务器则选中该设备对应的 IP 即可，反之则不必选中。

2. 查看认证服务器

用户可通过在 RADIUS 认证服务器管理界面中选中一个认证服务器，然后点击“查看”按钮进入认证服务器查看界面，查看认证服务器的配置信息，包括：

- 服务器 IP
- 共享密钥
- 最大重传数
- 最大发送失败数
- 服务器状态
- 重传时间间隔
- 最大重传丢弃数
- 服务器 ID
- 客户端 IP
- UDP 端口

注意

一次只能查看一条认证服务器的详细配置，若用户选中多条认证服务器，则查看按钮将灰化。

3. 删除认证服务器

用户可通过在 RADIUS 认证服务器管理界面中选中一个或多个认证服务器，然后点击“删除” 按钮即可删除选中的认证服务器。为确保安全删除，每次用户进行删除操作时都会有确认提示，若用户选择“否”则不继续进行删除操作；若选择“是”则删除所选认证服务器。

4. 修改认证服务器

用户可通过在 RADIUS 认证服务器管理界面中选中一个或多个认证服务器，然后点击“修改” 按钮进入认证服务器修改界面，修改选中的认证服务器配置，包括：

- 共享密钥
- 重传时间间隔

- 最大重传丢弃数
- 最大重传数
- 最大发送失败数

提示

当一条认证服务器创建完成以后，服务器 ID、服务器 IP、客户端 IP 以及 UPD 端口将不再允许用户进行修改，能修改的项只有共享密钥、重传时间间隔、最大重传丢弃数、最大重传数以及最大发送失败数五项。

设定好各项值之后单击“保存”按钮即可完成修改，成功或失败都会有提示。

单击“刷新”按钮可重新设定各个配置项。

5. 刷新

在 RADIUS 认证服务器管理界面中单击“刷新”按钮即可同步当前集群中的认证服务器数据。

5.18.4 计费服务器

用户可通过选择“特性” －>“RADIUS 管理” －>“计费服务器”菜单项，进入 RADIUS 计费服务器的管理界面，进行 RADIUS 计费服务器的创建、查看、修改、删除等操作。

计费服务器的配置和认证服务器差不多，不再赘述。只是计费服务器的 UDP 端口号默认是 1813。

5.18.5 属性配置

属性配置包括属性基本配置和属性表的配置。属性基本配置包括：

- 带宽单位：bps/kbps。
- 帧协议：从哪个属性值中带回帧协议
- NAS 端口类型：从哪个属性值中带回 NAS 端口类型
- 源 MAC 地址：从哪个属性值中带回源 MAC 地址

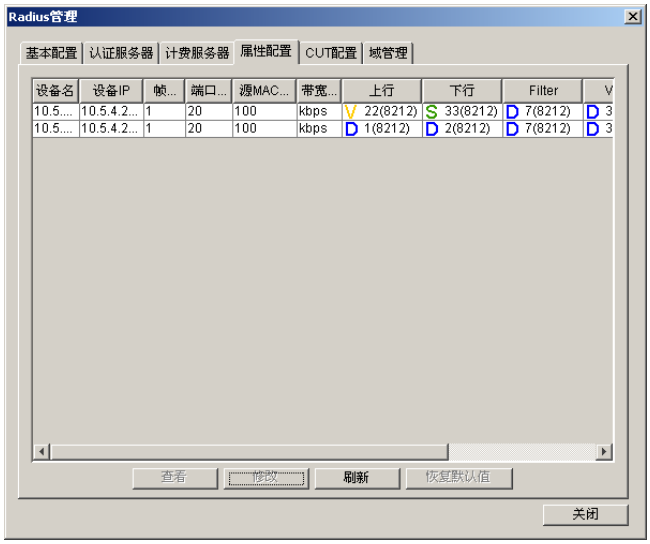
属性表的配置包括：

- 上行带宽
- 下行带宽
- Filter Id
- Vlan IP
- Vlan Id
- Path Track

每个用户参数有三项可配置：参数携带类型（使用标准属性、厂商自定义属性还是默认值）、属性值（用哪个属性带回用户参数）、厂商 ID。

用户可通过选择“特性” －>“RADIUS 管理” －>“属性配置”菜单项，进入 RADIUS 属性配置界面，如下图所示，中间显示了当前集群中所有设备的属性：

图5-40 属性配置



如上图所示，每一个属性参数采用图标和文字结合的方式来表示，例如：D 1(8212)。其中图标表示参数携带类型，其涵义如下：

- V —— 厂商自定义属性
- D —— 默认值
- S —— 标准属性

紧接着的数值为属性值，后面用括号括起来的为厂商 ID。

1. 查看属性

在 RADIUS 属性配置界面中选中一台设备，然后点击“查看”按钮进入 RADIUS 属性查看界面，如下图所示，查看 RADIUS 属性配置信息。

图5-41 查看属性

注意

一次只能查看一台设备的属性，若用户选中多台设备，则查看按钮将灰化。

2. 修改属性

在 RADIUS 属性配置界面中选中一台或多台设备，然后点击“修改”按钮即可进入修改属性界面，修改选中的设备。

属性配置包括属性基本配置和属性表的配置。其中属性基本配置包括：

- 带宽单位：bps/kbps。
- 帧协议：从哪个属性值中带回帧协议
- NAS 端口类型：从哪个属性值中带回 NAS 端口类型
- 源 MAC 地址：从哪个属性值中带回源 MAC 地址

属性表的配置要注意的是，如果欲设置参数携带类型为厂商自定义模式，必须设置属性值为非默认值。否则，系统将自动置参数携带类型为默认值模式。此外，当选择使用默认值时，属性值和厂商 ID 不允许设置。

设置好之后单击“保存” 按钮即可完成修改，成功或失败都会有提示。

单击“刷新” 按钮可重新设定各个配置项。

3. 恢复默认值

在 RADIUS 属性配置界面中选中一台或多台设备，然后单击“恢复默认值”按钮即可将所选设备的各属性恢复成默认值。

4. 刷新

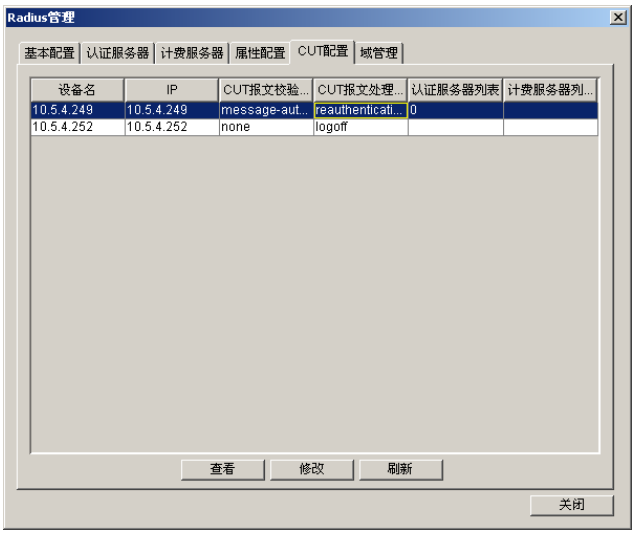
在 RADIUS 属性配置界面中单击“刷新” 按钮即可同步当前集群中所有设备的属性数据。

5.18.6 CUT配置

当由于某种原因 RADIUS Server 要求用户下线时，将发出一种 RADIUS 格式请求报文（CUT）给设备，设备一直在指定的 UDP 端口监听该请求。网络中可能存在多个 RADIUS Server，包括认证服务器和计费计费服务器，但是设备只准备处理某些服务器发出的 CUT 请求，于是管理员就要为设备配置一个 CUT 服务器列表，在此列表中存放着这些服务器的信息。

用户可通过选择“特性” －＞“RADIUS 管理” －＞“CUT 配置”菜单项，进入 RADIUS CUT 配置界面，如下图所示，中间显示了当前集群中所有设备的 CUT 配置，用户可对 CUT 配置进行查看、修改和刷新操作。

图5-42 CUT 配置



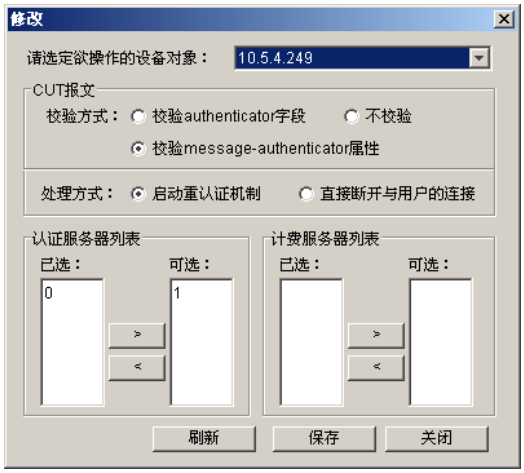
1. 查看 CUT 配置

在 RADIUS CUT 配置界面中选中一台设备，单击“查看” 按钮，将弹出查看 CUT 配置对话框，显示 CUT 配置，包括 CUT 报文校验方式、处理方式、认证服务器列表和计费服务器列表等信息。

2. 修改 CUT 配置

在 RADIUS CUT 配置界面中选中一台或多台设备，点击“修改”按钮进入 CUT 配置修改界面，如下图所示，修改选中设备的 CUT 属性。

图5-43 修改 CUT 配置



CUT 配置主要包括报文处理方式（校验方式和处理方式）、认证服务器列表和计费服务器列表。

报文处理校验方式有三种：

- 校验 authenticator 字段：校验 CUT 报文的 authenticator 字段
- 校验 message-authenticator 属性：校验 CUT 报文的 message-authenticator 属性
- 不校验，默认为不校验。

报文处理方式有两种：

- 启动重认证机制：设备将启动重认证机制处理 CUT 请求
- 直接断开与用户的连接：设备将直接断开与用户的连接

认证服务器列表左边为已选中的 CUT 认证服务器，右边为可选的 CUT 认证服务器，只需通过单击“>”和“< ”按钮即可方便的选择和删除 CUT 认证服务器，计费服务器的操作也是一样。

设置好之后单击“保存” 按钮即可完成修改，成功或失败都会有提示。

单击“刷新” 按钮可重新设定各个配置项。

3. 刷新

在 CUT 配置界面中点击“刷新”按钮即可同步当前集群中所有设备的 CUT 配置数据。

5.18.7 域管理

用户可通过选择“特性” －>“RADIUS 管理” －>“域管理”菜单项，进入 RADIUS 域管理界面，如下图所示，中间显示了当前集群中的所有域。

图5-44 域管理

1. 新建域

在 RADIUS 域管理界面中点击“创建”按钮，将弹出新建域的对话框。

创建很简单，只要指定域名即可，创建时可以指定在哪些设备上创建，只需要选中“选择设备”项即可，默认为非选中状态，则针对集群中所有设备进行配置。此外，还可以指定基本配置，若不指定则所有基本配置都采用默认值。各基本配置的含义如下：

- 认证状态：是否启动这个域的 RADIUS 认证，不影响其他域的认证。
- 认证类型：每个域都有三种认证类型：pap、chap、eap_md5。
- 认证模式：独立认证模式还是主备认证模式。独立认证模式是指当域内的 RADIUS 主认证服务器处于故障的时候，不把认证转移到域内的备份 RADIUS 认证服务器上；主备认证模式是指当域内的 RADIUS 主认证服务器出现故障的时候，交换机自动把认证切换到域内的备用 RADIUS 认证服务器上去认证。
- 完整用户名：需要还是不需要。是否带完整的用户名到 RADIUS 服务器。
- 计费状态：使能还是禁止这个域的计费，不影响其他域的认证。
- 计费模式：独立记账模式、主备记账模式还是多服务器记账模式。独立记帐模

式是指当 RADIUS 主记帐服务器出现故障的时候，交换机不主动把记帐信息发送到备用 RADIUS 记帐服务器上；主备记帐模式是指当 RADIUS 主记帐服务器出现故障的时候，交换机自动把记帐切换到备用 RADIUS 记帐服务器上；多服务器记帐模式是指在交换机记帐的时候，把一份记帐信息同时向多个 RADIUS 记帐服务器发送。

- 即时记账：使能还是禁止。即时记账功能(Interim Update Accouting)是在发送记账开始请求和记账结束请求之间定期发送即时记账请求，将在线用户的记账信息定期发送到 RADIUS 记账服务器。
- 记账间隔：当即时记账使能时的发送间隔，如果原先即时记账被禁止，则设此项可以打开即时记账功能。
- 是否需要 IP：需要还是不需要。即在发送计费请求报文之前是否获得用户的 IP 地址。
- 等待时长：根据命令行的配置，一段时间之后如果还没有得到 IP 地址，则根据超时机制，将切断该用户的连接。

2. 查看域

在 RADIUS 域管理界面中选中一个域，点击“查看” 按钮，将弹出查看域对话框，显示 RADIUS 域的配置信息。

注意

一次只能查看一个域的详细配置，若用户选中多个域，则查看按钮将灰化。

3. 删除域

在 RADIUS 域管理界面中选中一个或多个域，点击“删除”按钮即可删除选中的域。为确保安全删除，每次用户进行删除操作前都会有确认提示，若用户选择“否”则不继续进行删除操作；若选择“是”则删除所选域。

注意

默认域（default）不允许删除。

4. 修改域

在 RADIUS 域管理界面中选中一个或多个域，点击“修改”按钮即进入修改界面，可修改选中的域。

域的各个基本配置项均可修改。此外，还可以指定此域对应的计费服务器和认证服务器，若想将某个计费服务器加入到此域中来，只要选中该服务器前面的单选按钮即可。设定计费或认证服务器时需要指定此服务器以何种方式加入到此域中来。认证服务器有两种方式：首选或备份；计费服务器有三种方式：首选、备份或多服务器模式。

设定好之后点击“保存”按钮即可完成修改，成功或失败都会有提示。

注意

1、primary 服务器只有一个，当某服务器被指定为 primary 后，其它 primary 服务器将自动变成 backup。

2、当往某个域中加入服务器时，如果此域中还没有服务器，在新加入的服务器自动为首选，不管你设置的是何种类型。

5. 刷新

在 RADIUS 域管理界面中点击“刷新”按钮即可同步当前集群中的域及域的配置项。

5.19 NAS管理

5.19.1 概述

随着宽带以太网建设规模的迅速扩大，为了适应用户数量急剧增加和宽带业务多样性的要求，港湾网络有限公司通过在 Hammer 系列交换机上嵌入接入服务完成用户的认证和管理功能，以便更好地支持宽带网络的计费、安全、运营和管理的要求。嵌入了接入服务的 Hammer 交换机称为网络访问服务器（Network Access Server，NAS）。

接入服务在运用 802.1x 协议和 RADIUS 协议的基础上，实现对用户接入的认证和管理功能。使用接入服务主要有以下优点：

- **简洁高效**：纯以太网技术内核，保持 IP 网络无连接特性，去除冗余昂贵的多业务网关设备，消除网络认证计费瓶颈和单点故障，易于支持多业务；

- **容易实现**：可在普通 L3、L2、IP DSLAM 上实现，网络综合造价成本低；
- **安全可靠**：在二层网络上实现用户认证，并可以通过设备实现 MAC、端口、账户和密码等绑定技术，具有很高的安全性；
- **易于运营**：控制流和业务流完全分离，易于实现多业务运营。

接入服务在运用 802.1x 基于端口的访问控制协议的基础上扩展了该协议，实现了基于用户 MAC 地址的访问控制，可以对设备一个端口上的多个接入用户分别进行认证和管理，提供对用户接入的灵活控制，同时能够与动态主机配置协议中继代理（DHCP Relay）相结合，为计费服务器提供用户的 IP 地址。

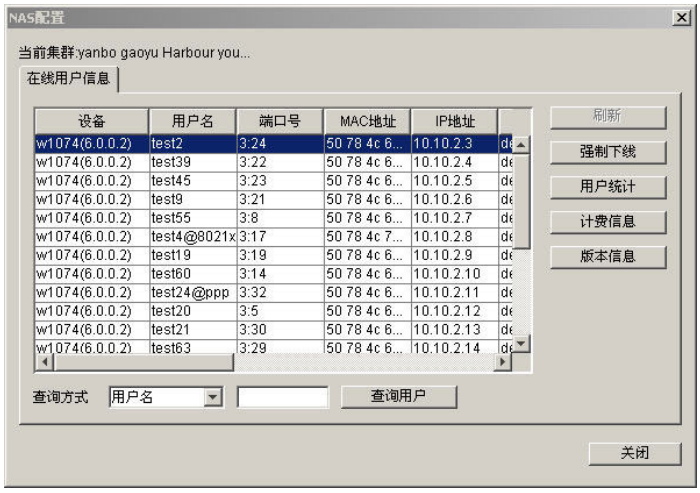
接入服务提供 3 种身份验证方式：PAP、CHAP 和 EAP-MD5 方式，根据业务运营的不同需求，可以使用其中任何一种身份验证方式实现接入服务。

UniWorks DSL Center 系统主要提供了 NAS 信息的查看功能。

5.19.2 在线用户信息

选择菜单项“特性－NAS 管理”，启动 NAS 管理功能，如下图所示：

图5-45 NAS 管理



系统列出所有在线用户的信息，包括用户名、端口号、MAC 地址、IP 地址、ISP 域、VLAN、状态、认证类型、PE 类型、注销原因、登录时间和在线时间。

单击“强制下线”按钮，可以强制用户为离线状态。

单击“用户统计”按钮，显示每个设备上的用户统计信息，包括设备、用户总数、

被使用的用户 ID、高端用户、正在认证的用户、已经认证的用户、等待 DHCP 的用户、等待计费响应的用户、在线用户、PAP 认证的用户、CHAP 认证的用户和 EAP MD5 认证的用户等信息。

单击“计费信息”按钮，显示每个设备上的计费相关信息，包括设备、开始计费时发送请求的数目、开始计费时收到响应的数目、停止计费时发送请求的数目和停止计费时收到响应的数目等信息。

单击“版本信息”按钮，显示每个设备的 NAS 版本号，包括设备和版本信息。

用户还可以对列出的在线用户信息进行查询操作，系统提供了六种查询类型：用户名、端口号、MAC 地址、IP 地址、ISP 域和 VLAN。

点击“查询用户”，显示查询结果，包括设备、用户名、端口号、MAC 地址、IP 地址、ISP 域、VLAN、状态、认证类型、PE 类型、注销原因、登录时间和在线时间等信息。

5.20 静态路由

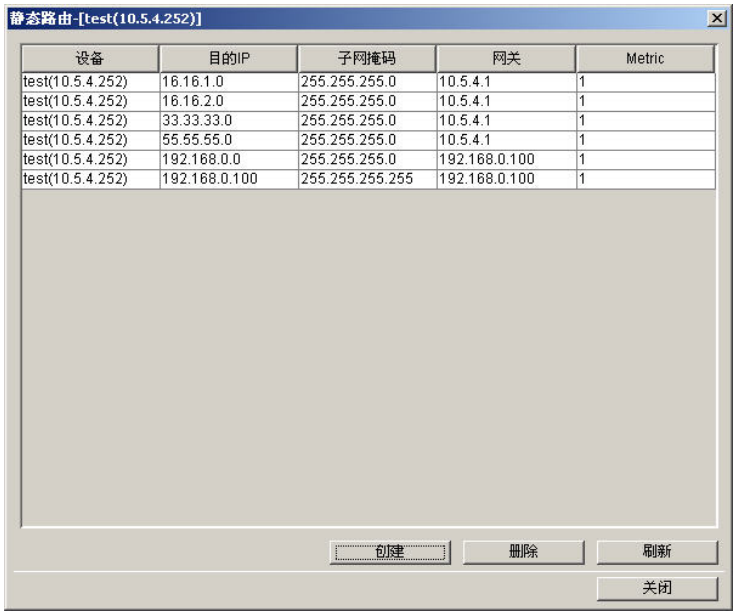
5.20.1 概述

静态路由是由用户定义的一条可使数据包从源地址通过指定路径到达目的地址的路由。当动态路由协议未能创建一条到特定目的的路由时，静态路由就显得尤为重要。还可以通过配置某一静态路由为默认路由，把无路由的数据包发送到默认的网关。

5.20.2 创建

选择一个或是多个设备对象，选择菜单项“特性－静态路由”，启动静态路由配置功能。系统首先列出所选设备上的静态路由表项，如下图所示：

图5-46 静态路由



单击“创建”按钮，启动静态路由表项创建功能，要求输入目标网络 IP 地址、子网掩码、网关地址和 Metric。

5.20.3 删除

选择一个或是多个路由表项，单击“删除”按钮，则删除这些表项。

5.20.4 刷新

单击“刷新”按钮，系统重新从所选的设备中获取静态路由信息。

5.21 访问控制

5.21.1 概述

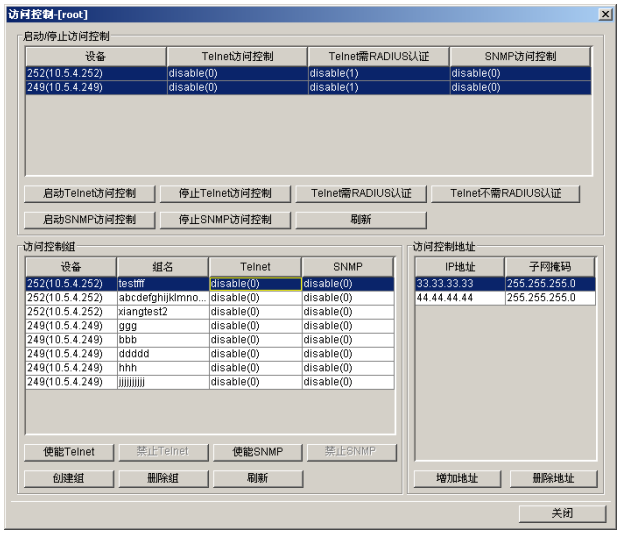
访问交换机有三种方式：命令行接口（CLI） 、远程登录(Telnet) 和简单网管协议

（SNMP）。对于后面两种方式的访问，可以通过相应的访问控制命令进行配置，以加强对交换机的访问控制管理。

访问控制是指网络管理服务（Network Management Service）的安全性，主要是用来设置 Telnet 和 SNMP 访问的权限，被禁止的 IP 或网段不能通过 Telnet 或 SNMP 访问交换机。

配置交换机的访问控制，必须先创建一个 NMS 访问控制组， 再配置相应的访问控制方式及 IP 地址。访问控制主界面如下图所示：

图5-47 访问控制



5.21.2 设备访问控制配置

设备访问控制包括 Telnet 访问控制的启动/停止、SNMP 访问控制的启动/停止以及配置 Telnet 访问控制是否需要 RADIUS 认证共三种操作。

只有启动了 SNMP 和 Telnet 访问控制，访问控制组的设置才能生效。

1. 启动/停止 Telnet 访问控制

选中设备名称（单选或多选），然后单击‘启动 Telnet 访问控制’或‘停止 Telnet 访问控制’，成功与否会有相应提示，同时在界面中刷新设置的结果。

2. Telnet 访问控制是否需要 RADIUS 认证

选中设备名称（单选或多选），然后单击‘Telnet 需 RADIUS 认证’或‘Telnet 不需 RADIUS 认证’，成功与否会有相应提示，同时在界面中刷新设置的结果。启动此功能的设备在 Telnet 登录此设备时，会需要 RADIUS 认证，只有 RADIUS 认证通过后方可成功登录

3. 启动/停止 SNMP 访问控制

选中设备名称（单选或多选），然后单击‘启动 SNMP 访问控制’或‘停止 SNMP 访问控制’，成功与否会有相应提示，同时在界面中刷新设置的结果。注意，在启动 SNMP 访问控制时，会有提示信息，提醒本系统可能会和设备失去连接。

注意

由于本系统是采用 SNMP 协议来管理设备，所以一般情况下，请不要启动 SNMP 访问控制，否则本系统会失去和设备的连通性。

5.21.3 访问控制组管理

1. 增加访问控制组

在访问控制主界面上的访问控制组区段，点击‘创建组’，会弹出创建控制组界面。

在访问控制组界面上，上部分为访问控制的组名，最长 19 个字符，下部分为选择在哪些设备上创建，默认为选择全部设备。

创建成功的访问控制组的访问属性：Telnet 和 SNMP 都是 disable，即此组内的 IP 地址都不允许 Telnet 和 SNMP 访问此交换机。

2. 删除访问控制组

选中要删除的访问控制组（可多选），点击‘删除组’，系统提示删除确认信息，点击‘是’即可，成功与否会有相应的提示信息。

3. 配置访问控制组

配置访问控制组包括设置访问控制组的访问属性，也包括向访问控制组添加或删除 IP 地址

(1) 设置访问控制属性

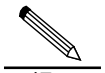
在访问控制主界面上，选中要设置的访问控制组，点击访问控制属性按钮（使能 Telnet、禁止 Telnet、使能 SNMP、禁止 SNMP）进行设置，成功与否会有相应提示信息。

(2) 添加访问控制 IP 地址

选中要配置的访问控制组（只能单选，多选或不选则添加按钮变灰），然后点击‘增加地址’，会弹出增加地址对话框，输入 IP 地址和掩码之后，点击‘确定’即可完成操作，成功的话，访问控制主界面上会有刷新，如果失败，会有提示。

(3) 删除访问控制地址

选中要配置的访问控制组（只能单选，多选或不选则添加按钮变灰），然后再选中要删除的 IP 地址（可以多选），点击‘删除地址’，系统弹出删除确认信息，点击‘是’即可完成操作，成功与否会有相应的提示信息。

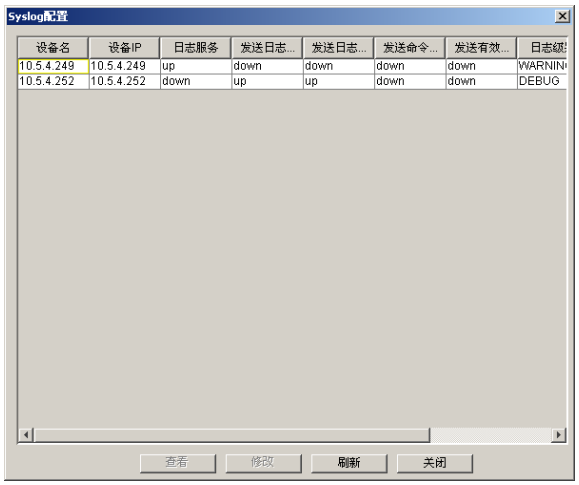

提示

虽然访问控制能够实时刷新数据，但还是在各个表的下面都提供了‘刷新’按钮，供用户手工刷新数据。

5.22 SYSLOG配置

SYSLOG 配置用于设置发送设备日志的相关参数。用户可通过选择“特性” －> “SYSLOG 配置”菜单项，进入 SYSLOG 配置管理界面，如下图所示：

图5-48 SYSLOG 配置



1. 查看 SYSLOG 配置

在 SYSLOG 配置界面中选中一台设备，点击“查看”按钮，将弹出查看 SYSLOG 配置对话框，显示日志服务器配置、日志功能设定以及日志类型等相关信息。

注意

一次只能查看一台设备的 SYSLOG 相关配置，若用户选中多台设备，则查看按钮将灰化。

2. 修改 SYSLOG 配置

在 SYSLOG 配置界面中选中一台或多台设备，点击“修改”按钮即可进入 SYSLOG 配置修改界面，用户可修改选中设备的 SYSLOG 配置。

SYSLOG 配置包括三部分：日志服务器配置、日志功能设定以及日志类型的配置。下面分别说明：

1）日志服务器配置

通过“增加”按钮，可增加接收 Syslog 的服务器。需要输入要增加服务器的 IP 地址、服务器端口号，以及文件索引，即指“Facility”，共有 local0 到 local7 八个选项，通过下拉列表选择。然后，单击“确定” 按钮，即增加了一个 Syslog 服务器。最多可增加 5 个服务器。

也可通过“删除” 按钮来删除 Syslog 的服务器。方法是：先选定要删除的条目，然后，单击“删除”按钮即可删除相应的服务器。

2）日志功能设定

日志功能设定包括如下六个功能项：

- 日志服务是否启动：设置代理 Syslog 服务启动/关闭。选择 up 启动，否则关闭。
- 日志是否发送至服务器：选择 Up，则 Syslog 日志可以发送到在日志服务表中已定义的服务器上，否则不能。
- 日志是否发送至终端监视器：设置 Up，Syslog 日志可以在终端监视上显示，否则，不能。
- 命令行是否发送至服务器：若选择 Up，则命令行也可发送至服务器。
- 有效命令是否发送至服务器：有些用户不想把正确的有效命令也发送至服务器，那么就可将此项设置为 Down。否则，发送。
- 日志级别：通过下拉列表有 8 种级别供您选择。

用户可以通过下拉列表对它们分别进行设置。

3）日志类型的配置

通过鼠标选定日志状态列的下拉列表可设置相应日志类型的状态(Up/Down)。目前支持的日志类型有 AUTH，CLI，SYSLOG，DEVCTRL，DOT1X，NAS，RADIUS，WEBAUTH，DHCPR，DHCPS，HIPMG，OSPF，PORT，RIP，ROUTE，SNMP，STP，SYSTEM，VLAN，L2SWITCH，TRACEROUTE，PORTB，GTDRV，FIREWALL，FDB，TIMER，TELNETF，PACKETDEBUG，FFS，PPPoE，PPP，DHCPC，ADSL，IGMPS，POS，ATM，L3SWITCH，ACLQOS，BOARD，FPGA，LOCALBUS，PNP，IPC，VDUB_DRIVER，DEBUGOUT 等。

3. 刷新

在 SYSLOG 配置界面中单击“刷新”按钮即可同步当前集群中所有设备的 SYSLOG 配置数据。

5.23 TRAP配置

选择一个或是多个设备对象，选择菜单项“特性－TRAP 配置”，启动 TRAP 配置功能。

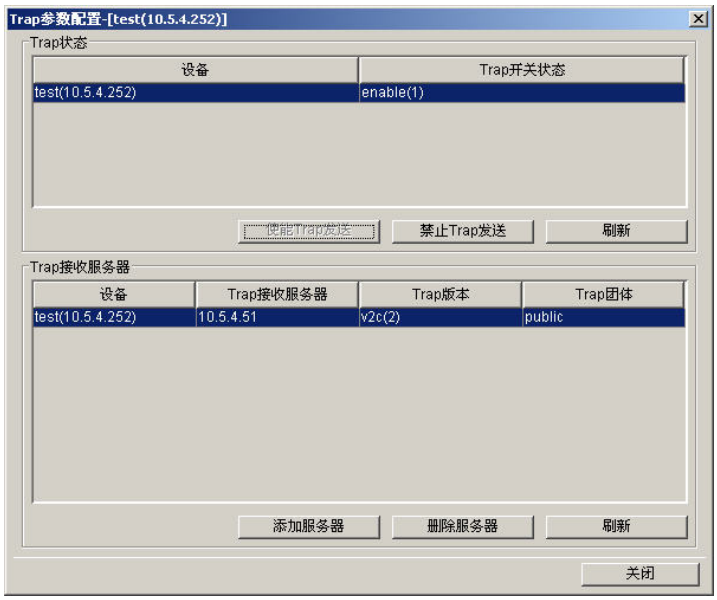
TRAP 配置包括两个部分的内容：

- Trap 状态：系统首先列出所选设备的 TRAP 开关状态。选中一个或是多个表项，单击“使能 TRAP 发送”按钮，启动 TRAP 发送功能；单击“禁止 TRAP 发送”，则关闭 TRAP 发送功能。单击“刷新”按钮，系统重新从设备上获取 TRAP 状态。
- Trap 接收服务器：单击“添加服务器”按钮，可以给设备添加 TRAP 接收服务器，包括配置接收服务器地址、TRAP 版本（v2c/v1）和 TRAP 团体（可不输入）。

单击“删除服务器”按钮，从设备上删除 TRAP 接收服务器的配置信息；单击“刷新”按钮，系统重新从设备上获取 TRAP 接收服务器信息。

例如，选择一个设备对象 test(10.5.4.252)，启动 TRAP 发送功能，并添加 TRAP 接收服务器 10.5.4.51，TRAP 版本为 v2c，TRAP 团体为 public，配置结果如下图所示：

图5-49 配置 TRAP



5.24 配置设备PVC服务

选择一个或是多个设备对象，选择菜单项“设备－配置设备 PVC 服务”，启动配置 PVC 功能。系统列出所选设备的 VPI 值和 VCI 值。

选择一个或是多个表项，单击“修改”按钮，可进入修改 PVC 界面，修改指定设备的 VPI 和 VCI 值。

5.25 广播抑制

本功能项主要是为了选择在某台设备上是否启用广播抑制功能，并设置广播抑制的相关参数。用户可通过选择“特性－广播抑制”菜单项，进入广播抑制配置界面，如下图所示：

图5-50 广播抑制

操作方式同其它功能项一样，欲查看交换机当前配置状态，只需选中想要查看的交换机，其配置信息即可在下半部分面板上显示出来。欲修改交换机当前配置信息，用户首先得选中欲配置的交换机，可以单选也可以多选。然后在下半部分的面板上设定配置状态，然后点击“保存”按钮即可完成修改，成功或失败都会有提示。

这里共有四个配置项：

- 广播抑制功能：设定交换机的广播抑制功能启动/关闭。选择 disable(1)启动，否则关闭。
- 时间窗口值：设定交换机广播抑制时间窗口的值，在 1-16 秒之间选择。
- 单位：指定计数单位为 packets 还是 bytes。
- 计数值：计数值为 1-4294967295 之间的值

5.26 二层PPPOE配置

二层 PPPOE 配置的配置模式和硬件有关。由于硬件的不同，该项配置有不同的配置模式。配置模式有 4 种：none、normal、better 和 best。best 配置模式的配置方式不同于 normal 和 better 配置模式，none 模式下不提供该项配置功能。

若用户选中的集群中包括配置模式为 none 的设备，或当用户选择的集群中设备的配置模式不一致时，将不能进行二层 PPPOE 配置或批量配置，系统将提示错误信息，告诉用户无法进行二层 PPPOE 配置，原因可能是：

- 所选择的集群中设备配置模式不一致；
- 所选择的集群中包含无法进行二层 PPPOE 配置的设备

若集群中所有设备的配置模式均为 normal 或 better，则相应的可配置项包括：

- 二层透传 PPPOE 用户名绑定功能（启用/不启用）
- BRAS 服务器的地址

若集群中所有设备的配置模式均为 best，则应该针对每台设备的每个 VLAN 进行二层 PPPOE 的相关配置，配置项包括：

- 二层透传 PPPOE 用户名绑定(启用/关闭)
- 非 PPPOE 包过滤(启用/关闭)

6 在线升级

6.1 概述

FTP（File Transfer Protocol，文件传输协议）是网络中进行文件传输的基本协议。本系统就是采用此协议来更新设备文件和保存设备文件的，共提供了两种升级和保存方式：

- 使用内置 FTP 服务器
- 指定 FTP 服务器

用户可通过菜单项“配置—在线升级”进入文件传输配置界面，进行在线升级的相关设置。

6.2 使用内置FTP服务器升级

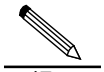
本系统内置了一个 FTP 服务器，它支持多客户端（最多 64 个）同时操作，因此提供了批量升级和批量保存功能。

注意

如果 PC 上已经启动了另外一个 FTP 服务器，则不能使用内置的 FTP 服务器。

可以在 FTP 目录中手工输入路径，也可以单击“设置 FTP 目录”来选择路径。系统默认为 C 盘根目录（第一次使用时），同时保存上次设置的值，以供下次使用。

当在 FTP 目录中手工输入的路径不是绝对路径时，系统默认为本系统的安装目录+手工输入的目录。


提示

为了保证路径的合法性，建议使用按钮“设置 FTP 目录”来选择路径。

6.3 指定FTP服务器

当指定其它的 FTP 服务器时，需要指定访问服务器的 IP、用户名称和密码。本系统不保证指定的服务器的连通性。

注意

如果指定的服务器不支持多客户端，则不能进行批量操作。如果指定的 FTP 服务器不支持多客户端而又进行了批量操作，则只是其中随机的某一台设备成功。

6.4 文件传输

6.4.1 参数设置

主要包括如下配置项：

- 操作类型：文件传输不仅可以下载设备文件（从主机到交换机），同时也可以上传设备文件（从交换机到主机）。
- 文件类型：共分为三种类型。其中 HammerOS 文件为交换机操作系统文件；配置文件为交换机的配置文件；XDUCODE 为 ADSL、VDSL 套片代码和 FPGA 代码合成文件。不提供 XDUCODE 文件上传功能。
- 文件名称：可以为每一台设备指定文件名称，也可以只指定一个基准文件。在下载设备文件时，如果指定一个名称，则用此文件下载到所有选定的设备中；在上传设备文件时，如果只指定一个文件名称，由于文件名称不能重名，为了便于区分，则系统会在每个上传成功的文件后面加上设备的标识。例如指定的基准文件名称为 a，设备名称为 252(10.5.4.252)，则上传的文件名称为：a_252(10.5.4.252)。

注意

文件名称最大为 30 个字符长度。

6.4.2 完成操作

设置完 FTP 参数后，点击“确定”即可进行操作，由于 FTP 操作需要一定的时间，所以鼠标处在等待状态，直到完成了操作，成功与否会有相应的提示，同时在主界面的操作结果中也会有操作结果的信息供用户查看。

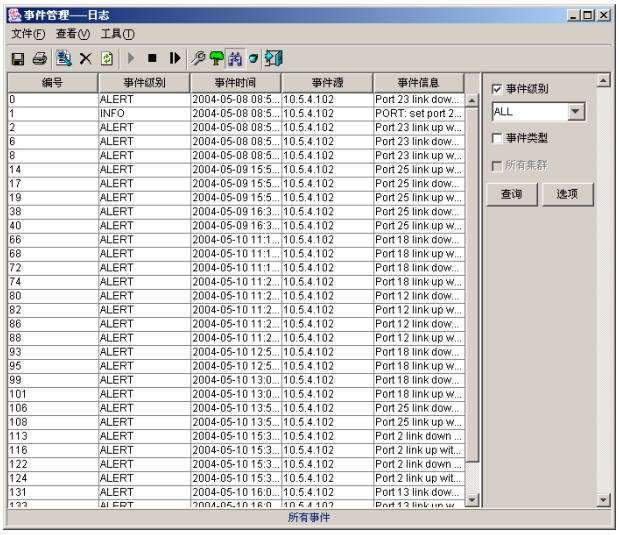
7 事件管理

7.1 概述

一个统一灵活、功能强大、可扩展的事件处理系统是一个网管系统的重要组成部分。借助这个事件系统，网络管理员和网管小组可以很容易的对网络中发生的重大事件进行监控，并采取适当的行动保持网络的健壮。而且网管系统本身也可以通过预配置的动作对重大事件做出反应，对网络进行自调整。UniWorks DSL Center 系统提供了统一的日志、告警事件管理界面，用户可以在同一个界面中同时管理所有的日志和告警事件。

用户可通过选择“配置” －>“事件管理”菜单项，进入事件管理界面，如下图所示：

图7-1 事件管理



7.2 文件菜单

文件菜单包括保存、打印和退出三个选项，在工具条中也设置了相应的快捷按钮，具体如下：

- 保存（S）：用于将事件管理页面表格中的事件保存为 Excel 格式的文件。用户可通过选择事件管理界面中的“文件” －>“保存”菜单项，然后确定保存文件的路径及文件名完成事件保存。
- 打印（P）：可以将事件管理界面表格中的事件打印出来。
- 退出（E）：退出事件管理。

7.3 查看菜单

查看菜单包括事件类型、清空事件库、事件详情、删除及刷新五个选项，在工具条内都设置了相应的快捷方式，具体如下：

- 事件类型（Y）：可以在日志管理和告警管理之间切换，若当前事件为日志事件则告警类型菜单为可用状态，若当前事件为告警事件则日志类型菜单为可用状态。
- 清空事件库（C）：用于清除所有已记录的事件并重启后台服务。选择“清空事件库”后，系统将提示确认信息。用户若选择“是”则执行清空操作；选择“否”则不执行清空。
- 事件详情（T）：查看一条事件的详细信息。但前提条件是已经选中一条事件；若没有选中事件，则弹出错误提示信息，提示用户选中一条事件查看。除了通过菜单和工具条操作外，用户还可以通过在一条事件记录上双击鼠标左键查看此事件的详细信息；或者选择鼠标右键菜单中的“事件详情”菜单项，查看此事件的详细信息。
- 删除（D）：用于将用户选中的事件从数据库中删除，前提是已经选中一条或多条事件；若没有选中事件，则弹出错误提示框，提示用户至少选择一条事件。在每次执行删除操作时，都会出现确认提示框，要求用户确认是否删除。若选择“是”则执行删除操作；选择“否”则不执行删除。除了可以通过菜单和工具条操作外，用户还可以使用鼠标右键菜单中的“删除”菜单项完成删除操作。
- 刷新（R）：用户通过选择“刷新”可以同步当前事件数据。

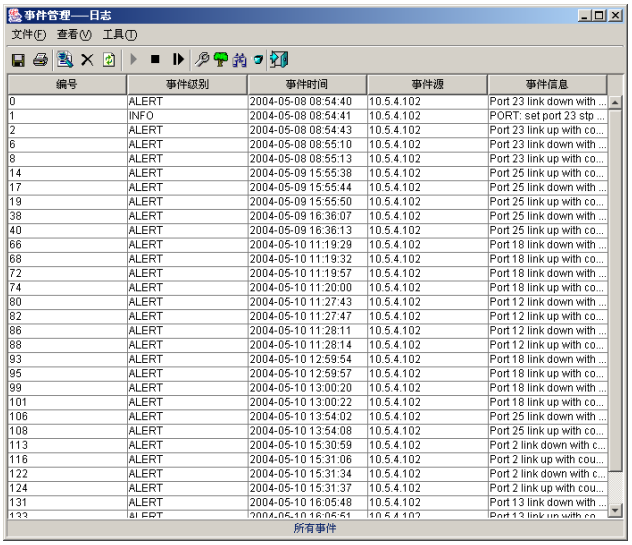
7.4 工具菜单

工具菜单包括搜索（S）、服务器配置（O）、SYSLOG 备份配置（B）、SYSLOG 服务（S）及 TRAP 服务（T）五个选项。除了 SYSLOG 服务选项，其它四项在工具条内都设置了相应的快捷方式。

7.4.1 搜索

用户通过选择“搜索”菜单可以打开、关闭搜索面板。关闭搜索面板后的管理界面如下图所示：

图7-2 关闭搜索面板



搜索面板包含各种搜索条件，用户可以通过这个面板自定义过滤条件，以便把您所关心的事件显示在一个特定的列表视图内。操作过程需要两个步骤：

1）输入过滤条件

2）单击“查询”进行检索

基本的搜索选项包括事件级别和事件类型两项，其中：

- 事件级别表示事件的严重程度，共有七个选项：ALL（所有级别）、EMERG、ALERT、WARNING、NOTICE、INFO 及 DEBUG。

- 事件类型共有两种：DslCenter（网管日志）及 HarbourDevice（设备日志）。若都不选则包括这两种类型。

单击“选项”按钮即可弹出其它高级过滤选项，其相关说明如下表所述。

表7-1 过滤选项说明

过滤选项	说明
事件名称	某一类型事件的简短名称
事件来源	表示事件发生的源IP地址 注：此字段支持通配符，支持用逗号分隔多个选项，例如下面的条件： 10.5.*，10.1.0.41，10.1.0.42 分别表示同时查询所有发源于10.5网段和10.1.0.41、10.1.0.42两个设备的事件
相关地址，相关用户	用于日志事件，表示日志相关的信息
事件详情	通过此条件可在事件详细信息字段中进行模糊查询
事件时间	表示事件发生的时间 注：指的是网管工作站接收到此事件的时间，应该和事件发生的原始时间区别开来。时间的格式比较灵活，例如以下格式均可识别： 20030227，2003-02-27，20030227141500，2003-02-27 14:15:00
原始时间	事件的原始发生时间 注：对于设备事件通常为设备的sysUpTime。

定义好过滤条件后，点击“过滤查看”按钮，系统将给出符合过滤条件的事件集。

7.4.2 服务器配置

用户通过“服务器配置”可以进行如下三项配置：

- 事件库限额：此选项用于设置事件库的事件数量，当事件数达到这个限额时，如果再有新的事件产生，则系统先删除事件库中最前面的事件，然后再存入新的事件。
- 日志最低级别：设置了日志最低级别后，对于低于此级别的事件，系统将不予接收。共包括 6 种日志级别：DEBUG、INFO、NOTICE、WARNING、ALERT、EMERG。
- Trap 任务：为了接收不同 SNMP 团体名甚至非 162 端口的告警信息需要配置多个告警任务。

完成配置后，点击‘应用’按钮使设置生效。点击‘清空事件库’按钮可以清空事件库里的所有事件。

注意

1、每个任务是一个 SNMP 团体名和端口用下划线连接起来的字符串，配置多个任务用逗号分隔。

2、public_162 是必须的任务，无论您如何配置，它都会被添加在您的任务配置中。

7.4.3 SYSLOG备份配置

系统还可以对 SYSLOG 记录进行备份，用户可以指定时间备份，也可以设定一个备份周期，单位为天。当周期到来时自动启动备份动作。用户可通过选择事件管理界面中的“工具”－>“Syslog 备份配置”菜单项进行备份配置，包括备份周期、预约时间和备份路径。

其中，预约时间是指第一次保存开始的时间，通过点击‘预约时间’按钮弹出对话框来配置。

用户可通过点击“浏览”按钮进行备份文件保存路径选择。最后单击备份配置界面的“确定”按钮即可启动自动备份功能。

7.4.4 SYSLOG服务

日志服务包括以下三项：

- 启动日志服务
- 停止日志服务
- 重新启动日志服务

用户可通过此菜单进行日志服务的启动、停止和重新启动。

7.4.5 TRAP服务

TRAP 服务包括以下三项：

- 启动 TRAP 服务
- 停止 TRAP 服务

- 重新启动 TRAP 服务

用户可通过此菜单进行 TRAP 服务的启动、停止和重新启动。

8 安全管理

8.1 概述

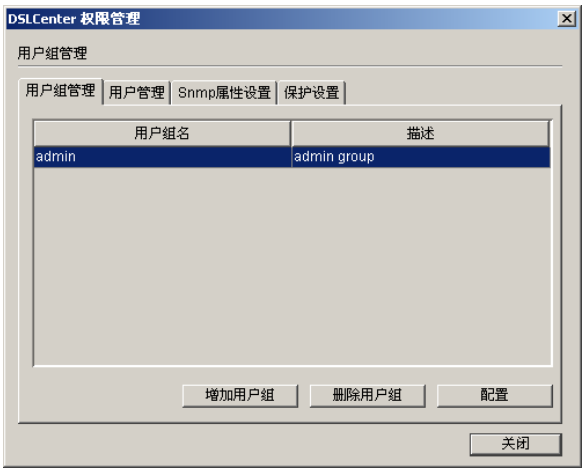
UniWorks DSL Center 系统提供了基于用户的安全管理。系统提供用户组和用户两个级别，每一个用户都必须隶属于一个指定的用户组。

通过 UniWorks DSL Center 系统提供的用户管理可以方便的创建用户组和用户，从而可以分别为每个用户组或用户指定不同的管理权限。安全管理同时也提供了设置设备访问团体的功能，只有本地设置的读写团体和设备上配置的读写团体一致时才能正确访问设备。同时只有 admin 用户组的用户才有权限登录安全管理，修改其他用户权限。

8.2 用户组管理

系统默认有一个用户组，名称为 admin，具有所有操作权限，不允许修改其权限，也不允许删除。用户组管理界面如下图所示：

图8-1 用户组管理



8.2.1 增加用户组

点击用户组管理界面中的‘增加用户组’按钮，弹出增加用户组对话框，输入组名和描述后，按‘确定’按钮即可。

组名长度要求在 20 个字符以内，只能是字母、数字和下划线的组合。描述可以为空。

新增加的用户组默认情况下具有所有功能的权限。

8.2.2 删除用户组

首先选中要删除的用户组，然后点击用户组界面中的‘删除用户组’按钮，系统弹出确认信息框要求用户确认。点击‘是’按钮将会删除选定的用户组。

注意

删除用户组会将组内所有的用户信息及用户授权信息全部删除。

8.2.3 配置用户组

首先选中要配置的用户组，然后点击用户组界面中的‘配置’按钮，系统弹出用户组配置对话框。

对于每个功能共分为三种权限：不提供、读取和读取&设置。如果是 admin 用户组的用户，则只有读取&设置权限。由于要支持批量操作，所以系统只提供按功能划分的权限管理。

8.3 用户管理

每一个用户都必须属于一个用户组，其权限就是所在组的权限，系统默认有一个属于 admin 用户组的超级用户 admin，默认密码为 harbour，密码可以修改。此用户不能删除。

提示

建议安装之后修改这个密码。

用户管理的界面如下图所示：

图8-2 用户管理

8.3.1 增加用户

点击用户管理界面中的‘增加用户’按钮，系统弹出增加用户界面，输入完用户名、密码、确认密码、描述等参数，并选定所属组后，点击‘确定’按钮即可。新创建的用户默认情况下状态是“激活”。

8.3.2 删除用户

首先在用户管理界面中选中要删除的用户，然后点击‘删除用户’按钮，系统会弹出提示信息框，要求用户确认，点击‘是’按钮将会删除选定的用户。

8.3.3 修改用户

首先在用户管理界面中选中要修改的用户，然后点击‘修改用户’按钮，系统弹出

修改用户对话框。

修改用户包括修改密码、用户所属组、用户状态和描述。修改了所属组后，用户的权限也就做了相应的改变。

当修改用户状态为“锁定”后，则此用户就不能再登录本系统，会提示相应信息：用户被锁定，请用超级用户解锁。

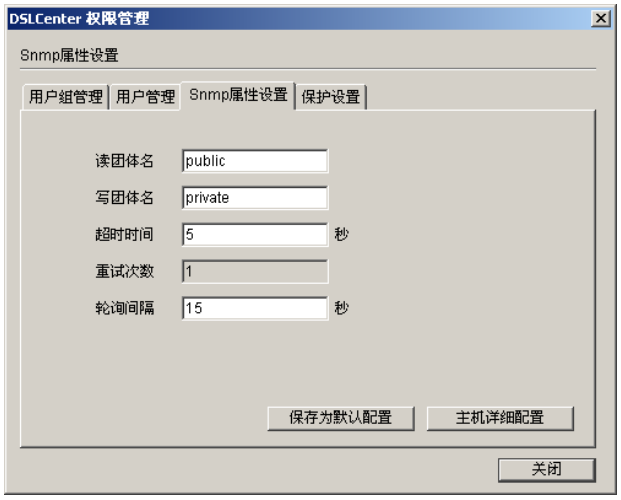
注意

当用同一个用户登录本系统失败三次后，系统会自动锁定此用户。

8.4 SNMP属性设置

SNMP 属性设置包括缺省属性配置和设备详细配置，只有当本地配置的读写团体和设备中的一致时，才可正确访问设备。当没有为一台设备配置本地 SNMP 属性时，使用缺省属性访问设备，SNMP 属性配置界面如下图所示：

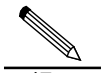
图8-3 SNMP 属性配置



8.4.1 默认配置

在 SNMP 属性配置界面上输入要配置的属性包括读团体名、写团体名、超时时间、重试次数和轮询间隔，然后点击‘保存为默认配置’即可。其中：

- 读团体名：能够读取设备信息时要提供的 SNMP 验证密码
- 写团体名：能够写设备信息时要提供的 SNMP 验证密码
- 超时时间：一次读/写操作设备没有相应的最大时间
- 重试次数：一次读/写操作失败后可以再次尝试的次数，系统设定为 1 次，不可修改
- 轮询间隔：读取设备信息时的刷新时间



超时时间乘重试次数应不小于轮询间隔。

8.4.2 主机详细配置

如果不是每个设备的 SNMP 属性都要求一致，则应该配置主机详细配置，它允许为每个设备配置其自己的 SNMP 属性，配置属性和默认配置的属性一致，只是还必须指定设备的 IP 地址。

当然，如果对此设备要使用默认的 SNMP 属性，只需从主机详细配置列表中删除即可。

8.5 保护设置

系统提供了另一种保护措施，当系统空闲不用一段时间之后，它会自动选择用户预先设置好的措施启动保护。

用户可通过保护设置界面进行保护类型和等待时间的设置。其中：

保护类型分为如下三种：

- 无：不启动保护
- 锁定：当空闲指定的时间段后，系统会自动被锁定，此时不能做任何操作。当在系统上移动鼠标时，会提示输入用户名和密码
- 退出程序：当空闲指定的时间段后，系统会自动退出。在退出时弹出对话框提

示用户系统即将推出

等待时间是指在启动保护措施之前系统空闲的时间，单位为分钟，默认为 10，可输入范围为 1-35791，只有保护类型为锁定和退出时才能设置等待时间。

9 业务配置向导

9.1 概述

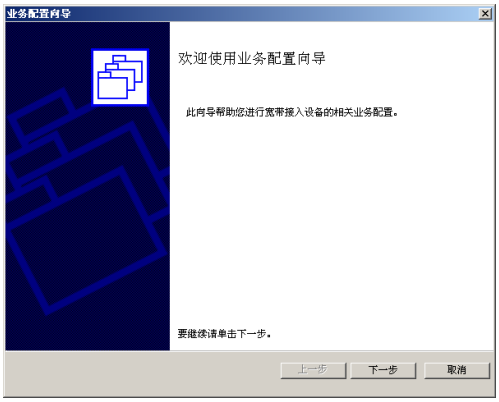
UniWorks DSL Center 系统提供了业务配置向导，用户可在向导提示下，完成相应的业务配置操作。

9.2 业务配置向导使用

9.2.1 启动业务配置向导

用户可通过选择“配置”－>“业务配置向导”菜单项启动业务配置向导，如下图所示：

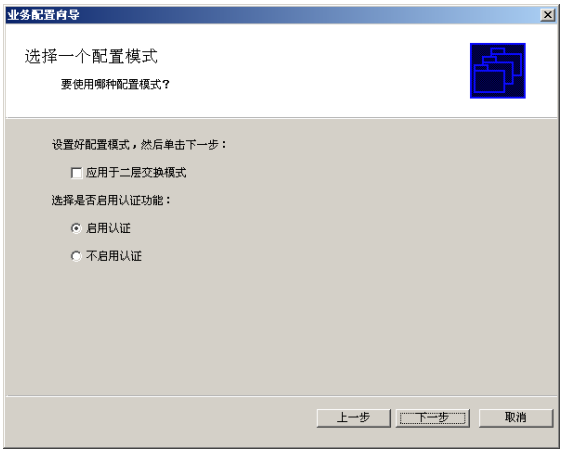
图9-1 欢迎使用业务配置向导



9.2.2 选择配置模式

单击“下一步”按钮，进入选择配置模式界面如下：

图9-2 选择一个配置模式



用户可根据需要选择是否应用于二层交换模式及是否启用认证功能。

9.2.3 二层透传配置

如果用户在选择配置模式界面中选择“应用于二层交换模式”及“不启用认证”，然后单击“下一步”按钮，则进入二层透传配置，界面如下：

图9-3 二层透传配置

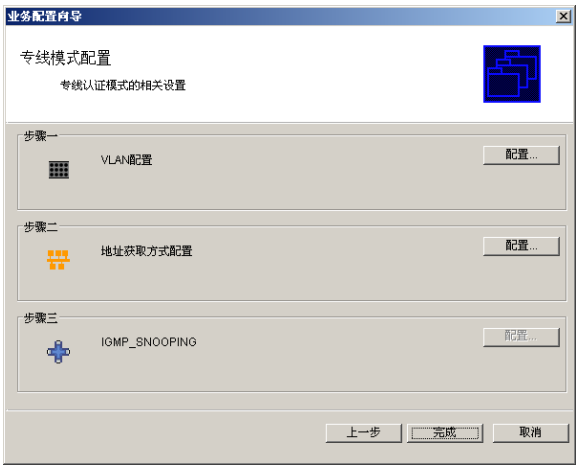
用户可根据向导按步骤完成相关配置后，单击“完成”按钮结束配置，并退出业务配置向导。

如果用户单击“上一步”按钮则返回上一级界面；如果选择“取消”按钮则中止当前的配置操作，并退出业务配置向导。

9.2.4 专线模式配置

如果用户在选择配置模式界面中不选择“应用于二层交换模式”及“不启用认证”，然后单击“下一步”按钮，则进入专线模式配置，界面如下：

图9-4 专线模式配置



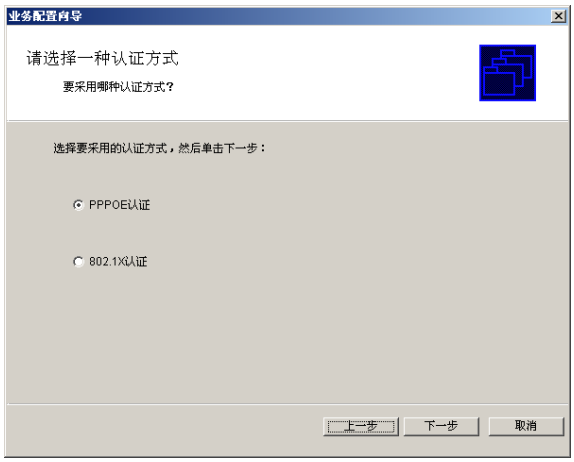
用户可根据向导按步骤完成相关配置后，单击“完成”按钮结束配置，并退出业务配置向导。

如果用户单击“上一步”按钮则返回上一级界面；如果选择“取消”按钮则中止当前的配置操作，并退出业务配置向导。

9.2.5 认证方式配置

如果用户在选择配置模式界面中选择了“启用认证”，则还需要指定采用哪种认证方式，单击“下一步”按钮后出现界面如下：

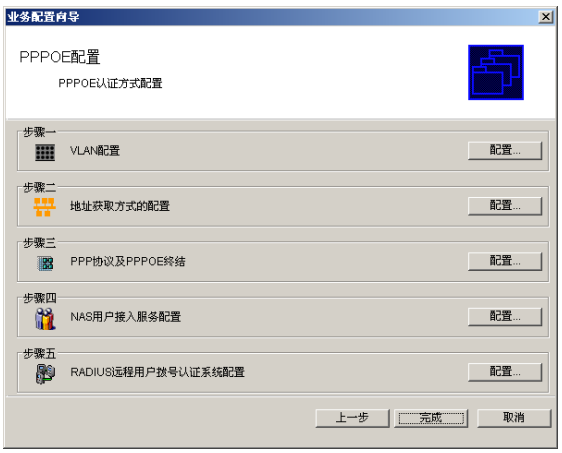
图9-5 选择认证方式



1. PPPOE 认证方式配置

如果用户在选择认证方式界面选择了“PPPOE 认证”，单击“下一步”按钮后进入 PPPOE 认证方式配置界面如下：

图9-6 PPPOE 认证方式配置



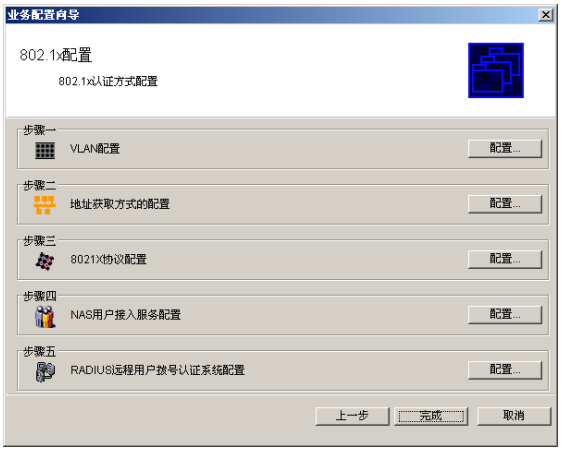
用户可根据向导按步骤完成相关配置后，单击“完成”按钮结束配置，并退出业务配置向导。

如果用户单击“上一步”按钮则返回上一级界面；如果选择“取消”按钮则中止当前的配置操作，并退出业务配置向导。

2. 802.1x 认证方式配置

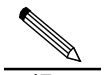
如果用户在选择认证方式界面选择了“802.1x 认证”，单击“下一步”按钮后进入 802.1x 认证方式配置界面如下：

图9-7 802.1x 认证方式配置



用户可根据向导按步骤完成相关配置后，单击“完成”按钮结束配置，并退出业务配置向导。

如果用户单击“上一步”按钮则返回上一级界面；如果选择“取消”按钮则中止当前的配置操作，并退出业务配置向导。


提示

有关业务配置的详细说明请参见前面章节的相关内容。

附录 A 系统管理和维护

UniWorks DSL Center 系统是为港湾网络有限公司的 Hammer10000 提供集群管理的软件产品。为了使 UniWorks DSL Center 系统能够正常运行，请用户在系统管理和维护时，注意以下几个方面的问题：

- UniWorks DSL Center 系统的 V1.00 版本只支持港湾网络有限公司 Hammer10000 设备 V2.00 及以上版本的集群管理。
- 被管理的设备必须有 snmp-agent 服务，并且已经被启动。
- 网管站与设备的网络连接正常，网管工作站和设备之间的 SNMP 协议报文能够正常通信。通常监测的办法是 Ping 被管理设备，进而通过第三方软件如 mib-browser 查看 SNMP 报文是否能够正常通信。
- 检查被管理设备的 agent 访问 community 是否和 UniWorks DSL Center 系统中设定的 community 相同。如果不同，则将 UniWorks DSL Center 系统中的 community 修正与设备 agent community 相同。
- 如果要利用 UniWorks DSL Center 系统监测网络告警，在设备上请配置网管工作站的 IP 地址为 Trap 接收地址。
- 如果要利用 UniWorks DSL Center 系统监测设备运行日志，在设备上请配置网管工作站的 IP 地址为 Syslog 的接收地址。
- 在集群管理中，如果有设备不通，则部分操作会很费时，请稍等一会。
- UniWorks DSL Center 系统不提供任何计费服务功能。

附录 B 常见问题处理

1. 查看后台服务状态

UniWorks DSL Center 系统的正常运行需要后台服务的支撑，查看这些服务状态可以判断是否正确安装，确定 UniWorks DSL Center 系统能否正常使用。

Windows 系统下查看 UniWorks DSL Center 系统服务运行状态的方法是：选择‘开始’—>‘设置’—>‘控制面板’—>‘管理工具’—>‘服务’，打开‘服务’。如果正确安装了 UniWorks DSL Center 系统，就会有“EasyTouch Event Service”和“MySql”两项服务，服务状态为“已启动”，启动类别为“自动”。

注意

不要手工修改这两项服务。如果服务不正常，请重启 Windows 系统或者卸载 UniWorks DSL Center 系统后重新安装。

2. 界面长时间没有响应

操作过程中如果出现界面长时间没有响应的情况，则可能是设备连通状况出现问题，请检查设备是否正常连通。

如果设备连通正常，则判断设备的读、写团体是否和本地配置的一致，也可以通过 UniWorks DSL Center 系统的菜单项‘工具’—〉‘启动轮询’来查看设备是否连通。

3. Trap 接收器里接收不到设备的 Trap

Trap 接收器里接收不到设备的 Trap，原因可能有如下五个：

- 本地的 MySql 服务没有正常启动，可对系统重新启动；
- 网管站与设备连接不正常，请保证设备能被网管站 ping 通；
- 设备的 Trap 服务未启动，请进入命令行启动 Trap 服务；
- 设备未配置网管站地址为接收 Trap 的地址之一，请进入命令行添加配置；
- 设备的 Trap 团体名不为 public，请进入告警监视窗口进行设置。